UNIVERZITA KARLOVA

Právnická fakulta

Daniel Oborák

Trestněprávní a kriminologické aspekty šíření ransomware

Diplomová práce

Vedoucí diplomové práce: doc. JUDr. Bc. Tomáš Gřivna, Ph.D.

Katedra: Katedra trestního práva

Datum vypracování práce (uzavření rukopisu) : 10. 9. 2021

Prohlašuji, že jsem předkládanou diplomovou práci vypracoval samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 188 302 znaků včetně mezer.

Daniel Oborák

V Praze dne 10. 9. 2021

Rád bych na tomto místě poděkoval doc. JUDr. Bc. Tomáši Gřivnovi, Ph.D., za jeho cenné rady a za odborné vedení této práce. Dále děkuji svým přátelům a rodině, jmenovitě Petru Rálišovi a Ing. Davidu Broniekovi za podnětné připomínky a návrhy. V neposlední řadě děkuji své přítelkyni, Martině Drozenové, za její trpělivost a podporu při psaní této práce i v průběhu celého studia.

Obsah

Úvod

S neustále se zvyšujícím významem internetu pro běžný život jednotlivce i pro chod společnosti jako celku se zvyšují rovněž rizika nevyhnutelně spojená s jeho základním atributem, kterým je rychlá, snadná a dostupná komunikace mezi jakýmikoliv zařízeními kdekoliv na světě. Kybernetická kriminalita, která byla po dlouhou dobu na okraji zájmu nejen kriminologického a trestněprávního[1], ale i zájmu celospolečenského či politického, je dnes považována za jednu ze zásadních hrozeb ohrožujících nejen partikulární zájmy jednotlivců či skupin, ale rovněž zájmy celospolečenské, tedy zájem na bezpečnosti České republiky, na řádném fungování kritické infrastruktury, na poskytování zdravotní péče, na řádném fungování veřejné správy a další.[2]

Tato práce se zabývá jedním z konkrétních projevů těchto tendencí, kterým je útok prostřednictvím šíření škodlivého kódu označovaného jako ransomware. Téma šíření ransomware jsem zvolil z důvodu jeho mimořádné aktuálnosti. V posledních letech doznal právě tento trend značné expanze, a to nejen po stránce kvantitativní, ale i po stránce technické a co do způsobu útoku. Ransomware útoky jsou dnes častěji zacílené na konkrétní subjekty s konkrétním záměrem a bývají mnohem více sofistikované, než tomu bylo v minulých letech.[3] K masivnímu rozšíření ransomware útoků po celém světě přispěla také globální pandemie onemocnění COVID-19.

Cílem této práce je kriminologický popis fenoménu šíření ransomware s důrazem na otázku etiologie tohoto jevu a na kriminologický popis osoby pachatele při aplikaci obecných i specifických kriminologických teorií, dále na viktimologickou a prevenční stránku řešeného problému, na otázku latence tohoto typu kriminality a na význam aktuálního světového dění na danou problematiku. Dále je cílem této práce trestněprávní kvalifikace jednotlivých typů ransomware útoků. Dílčím cílem je pak vlastní hodnocení současné právní úpravy trestního práva hmotného ve vztahu k tomuto fenoménu a představení konkrétního návrhu *de lege ferenda*.

Co se týče metodologie použité v této práci, primární metodou je rešerše zahraniční i české odborné literatury, zpráv a stanovisek veřejných institucí a orgánů státu, internetových zdrojů a

---

[1] KRUPIČKA, Jiří. *Trestněprávní a kriminologické aspekty internetové kriminality*. Praha, 2012. Disertační práce. Univerzita Karlova, Právnická fakulta. Vedoucí práce prof. JUDr. Jiří Jelínek, CSc., s. 8.
[2] Národní úřad pro kybernetickou a informační bezpečnost ČR. *Zpráva o stavu kybernetické bezpečnosti ČR - 2019* [online]. [cit. 2021-4-19]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/NUKIB_ZSKB_2019.pdf
[3] Tamtéž.

judikatury. Rešeršované informace budou následně podrobeny analýze, syntéze, typologické metodě a srovnávací metodě, na základě kterých budou učiněny závěry vlastní.

Práce je rozdělena na tři části. V první části se zabývám obecným úvodem do problematiky kybernetické kriminality a ransomware, uvádím zde definice některých základních pojmů a vymezení jednotlivých typů ransomware podle rozdílů v jejich funkcionalitě. Rovněž se v první části zabývám otázkou, zda je vůbec právní regulace a vymáhání práva státem, zejména pak v kontextu trestního práva, v kyberprostoru legitimní.

Ve druhé části se zabývám kriminologickými aspekty šíření ransomware, především otázkami vzniku tohoto fenoménu a otázkou, kdo je pachatelem tohoto typu kriminálního jednání. Součástí tohoto rozboru je rovněž představení některých kriminologických teorií, zejména pak tzv. *space transition theory*, a jejich aplikace na zkoumaný fenomén. Následuje kriminologický rozbor oběti ransomware, rovněž jsou nastíněny možnosti prevence tohoto typu kriminality. Následuje analýza šíření ransomware zaměřená na aktuální problémy a výzvy, příkladem budiž vliv již zmiňované globální pandemické situace na řešený fenomén, útoky na nemocnice, které jsou v současné době velmi častým a nebezpečným fenoménem, dále pak rozebírám specifika politicky motivovaných ransomware útoků či problematiku kybernetické války.

Ve třetí části se zabývám trestněprávní kvalifikací šíření ransomware, a to s ohledem na různé typy ransomware, které byly vymezeny v obecné části této práce, následuje kritická analýza současné právní úpravy. Závěrem se pokouším nastínit vlastní konkrétní návrh *de lege ferenda*.

Vzhledem k právnímu a kriminologickému zaměření práce se pokusím vyvarovat technicistnímu výkladu a zaměřím se především na kriminologicky a trestněprávně významné aspekty dané problematiky. To se týká například vymezení samotného pojmu ransomware a jeho jednotlivých typů, kdy jistě nelze odhlédnout od některých podstatných technických aspektů tohoto jevu, nicméně není potřeba uvádět definice za použití technických specifik, které jsou z hlediska kriminologického poznání a trestněprávní kvalifikace bez významu.

1 Úvod do problematiky kybernetické kriminality a ransomware

V první řadě je nutné zabývat se významem některých pojmů, se kterými bude v této práci dále nakládáno. Objasnění alespoň základních a nejpoužívanějších pojmů považuji za potřebné mimo jiné vzhledem k samotnému předmětu práce, kdy se v rámci studia kybernetické kriminality a šíření ransomware nelze vyhnout užívání pojmů technického charakteru, cizojazyčných pojmenování a mnohdy i internetového slangu. Nekladu si přitom za cíl nalézt vyčerpávající a všeobecně příjmané definice každého ze jmenovaných termínů, takový cíl by byl nedosažitelný, jelikož pojmy používané v oblasti kybernetické kriminality jsou často do jisté míry pohyblivé a i v rámci odborné literatury se lze setkat s odlišným chápaním konkrétního pojmu či s alternativním pojmenováním jednoho fenoménu.

1.1 Kyberprostor

Jaishankar ve svých přednáškách poněkud poeticky přirovnává kyberprostor k *Trishankovu nebi*, příběhu obsaženém ve starověkém indickém eposu *Rámájana*, který pojednává o králi *Trishanku*, jenž si chtěl do nebe přinést vlastní fyzické tělo, ale kvůli odporu boha nebes *Indry* mu bylo mocným mudrcem vytvořeno nebe vlastní, ve kterém se vznáší hlavou směrem k zemi. Je to jakási paralelní sféra, která není materiálním světem, ale která není ani opravdovým nebem.[4]

Kyberprostor lze skutečně označit, byť lehce nadneseně, jako jakýsi paralelní svět ke světu fyzickému. Je tvořený virtuálním prostředím, používaný a obývaný jednotlivými uživateli, kteří jsou připojeni a vzájemně propojeni prostřednictvím sítí elektronických komunikací. Významným znakem kyberprostoru je pak absence centrální autority nad tímto prostředím. I jako čistě virtuální svět však přináší do fyzického světa mnohé důsledky, včetně důsledků významných z pohledu trestního práva.[5]

[4] *What can human behavior online suggest about cyber crime | Jaishankar Karupannan | TEDxNITTrichy*. YouTube [online]. [cit. 2021-4-19]. Dostupné z: https://www.youtube.com/watch?v=Oiv6VK-FjAc

[5] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ, Ivana a kol. *Kriminologie. 5. aktualizované vydání*. Praha: Wolters Kluwer ČR, 2019. ISBN 978-80-7598-554-5, s. 388.

Pojem **kyberprostor** (ang. *Cyberspace*) původně vznikl pro potřeby *science fiction* beletrie, v rámci subžánru *cyberpunk*[6], poprvé jej použil spisovatel William Gibson v povídce *Burning Chrome* vydané v roce 1982 v časopise *Omni*. K širší popularizaci tohoto pojmu však došlo až následně, a to po vydání románu téhož autora nazvaném *Neuromancer* vydaném v roce 1984. V tomto románu Gibson rozvíjí představu o kyberprostoru jako o konsensuální halucinaci, virtuální realitě vytvořené ze shluků dat.[7]

Slovníková definice kyberprostoru jako pojmu beletristického, se kterou se můžeme setkat, říká, že jde o *„soubor veškerých dat uložených a veškeré komunikace vedené v počítačové síti, který je vnímán, jakoby měl vlastnosti fyzického světa"* či o *„prostředí virtuální reality"*.[8]

Populárně kulturní kořeny kyberprostoru nejsou patrné pouze v etymologii jeho pojmenování, ale odrážejí se rovněž v základním ideovém rámci[9], ve kterém byl kyberprostor rozvíjen zejména v raných dobách internetu. Výrazným projevem existence ideového zakotvení kyberprostoru bylo vydání textu „*A Declaration of the Independence of Cyberspace*"[10] Johnem Barlowem, zakladatelem *Eletronic Frontier Foundation*. Právě John Barlow začal pojem kyberprostor užívat ve vědeckých kruzích. Barlow na rozdíl od Gibsona vnímal pojem kyberprostor jako pojem výrazně širší, za kyberprostor označoval jakýkoliv deteritorializovaný a symbolický prostor mediované komunikace, přičemž pokročilost technologie determinuje komplexitu takového systému.[11] Za kyberprostor by tak dle Barlowa bylo možné označit například i telefonní síť.

V české legislativě, konkrétně v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů, nalezneme následující definici pojmu *kybernetický prostor* pro potřeby tohoto zákona: *„kybernetickým prostorem [se rozumí] digitální prostředí umožňující vznik,*

---

[6] Jedná se o subžánr science fiction, je charakteristický popisem technologicky a vědecky vyspělé civilizace spojené s rozpadem či zásadní změnou společenského řádu. Zdroj: *Kyberpunk*. Wikipedia [online]. [cit. 2021-4-19]. Dostupné z: https://cs.wikipedia.org/wiki/Kyberpunk

[7] Je vhodné podotknout, že k vydání těchto děl došlo před vznikem *world wide webu*, tedy před masivní expanzí sítě internet.

[8] PRUCHER, Jeff. *Brave New Words: The Oxford Dictionary of Science Fiction*. Oxford; New York: Oxford University Press, 2007. ISBN 0-19-530567-1, s. 31, přeloženo autorem z angličtiny.

[9] O přirozeném vzniku hodnotových rámců v informační společnosti pojednává: POLČÁK, Radim. *Autoritativní regulace kyberprostoru a legitimita trestního práva*. In GŘIVNA, Tomáš, POLČÁK, Radim. *Kyberkriminalita a právo*. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4, s. 12 – 25.

[10] BARLOW, John Perry. A *Declaration of the Independence of Cyberspace* [online]. [cit. 2021-5-30]. Dostupné z: https://www.eff.org/cyberspace-independence. V českém jazyce viz KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-18-8. s. 43.

[11] MACEK, Jakub. Kyberprostor. Revue pro média [online]. [cit. 2021-05-07]. Dostupné z: http://rpm.fss.muni.cz/Revue/Heslar/kyberprostor.htm

zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací".

Kolouch uvádí jako znaky kyberprostoru jeho decentralizovanost, globálnost, otevřenost, informační bohatost a interaktivnost. Z pohledu kriminologie a práva je nezanedbatelným aspektem kyberprostoru existence dopadů v reálném světě. Kolouch rovněž uvádí neoodělitelnost kyberprostoru a moderních technologií a existenci virtuální identity uživatelů označované jako *avatar.*[12] Dle Kudrlové je *avatar* do určité míry projekcí uživatele ve virtuálním prostoru, jeho účelem je přiblížení pohybu ve virtuálním prostředí reálnému prožitku.[13] Kudrlová *avatara* popisuje především optikou videoher[14], kdy je z pohledu uživatele (hráče) pochopitelná potřeba maximalizovat prožitek ze hry[15] prostřednictvím „vtělení" se do ovládané postavy. Tento jev však není výsadou videoher, pod avatary uživatelé vystupují rovněž na sociálních sítích, diskusních fórech a na seznamovacích webech. Z pohledu kriminologie lze považovat avatara za kriminogenní faktor[16], kdy se uživatelé pod anonymní či domněle anonymní identitou dopouštějí trestné činnosti, které by se pod svou skutečnou identitou nedopustili[17], či je avatar naopak předmětem kybernetického útoku.

Dle Gřivny kyberprostor zahrnuje veškerý virtuální prostor, především svět internetu, jiných sítí a mobilních technologií. Dále jej vymezuje funkcionálně, přičemž uvádí, že slouží jako komunikační platforma, informační zdroj, prostor pro informační systémy soukromých subjektů i veřejné správy. Rovněž slouží jako datové úložiště, pracovní prostředí, zábavní platforma a komerční zóna.[18] Z hlediska předmětu této práce je pak významné, že slouží rovněž jako prostor pro společensky škodlivé jednání.

---

[12] KOLOUCH, Jiří. *CyberCrime*. 2016. op. cit. s. 46.
[13] KUDRLOVÁ, Kateřina. *Avatar jako kriminogenní faktor*. In: SVATOŠ, Roman, KŘÍHA, Josef. (eds.) *II. kriminologické dny*. České Budějovice: Vysoká škola evropských a regionálních studií, 2014. ISBN 978-80-87472-65-1. s. 109 – 110.
[14] Zejména v rámci her žánru MMORPG („massively multiplayer online role-playing game"). Jde o hry, které asi nejlépe odpovídají představám cyberpunkové literatury o virtuální realitě. Jedná se o hry umožňující připojení masivního počtu hráčů najednou, zahrnující prvky her na hrdiny a kladoucí důraz na sociální interakci mezi hráči.
[15] Lze použít herním průmyslem často používaný pojem *immersion*, volně přeloženo z angličtiny jako *ponoření se do hry*.
[16] KUDRLOVÁ, K. *Avatar jako kriminogenní faktor*. 2014. op. cit. s. 111.
[17] O vlivu anonymity kyberprostoru na kriminální chování uživatelů internetu pojednávám níže.
[18] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ, Ivana a kol. *Kriminologie. 5. aktualizované vydání*. 2019. op. cit. s. 388.

1.1.1 Legitimita státní regulace kyberprostoru

Barlow v již zmiňovaném textu *A Declaration of the Independence of Cyberspace*[19] z roku 1996 vyjádřil myšlenku, že kyberprostor nemá být omezován jakoukoliv regulací ze strany jednotlivých států. Podle Barlowa státní moc, která existuje na základě vůle jeho obyvatel, nemá dosah do kyberprostoru, jelikož v kyberprostoru neexistuje společná vůle na podřízení se centrální autoritě, a stát tak nemůže nad jeho uživateli (respektive nad jejich virtuálními identitami) uplatňovat svou moc. Kyberprostor jako paralelní společnost byl podle něj vytvořen na základě nové společenské smlouvy.[20] Deklarace svým názvem, obsahem i ideovým zakotvením zjevně odkazuje na *Deklaraci nezávislosti Spojených států amerických* z roku 1776. V Deklaraci se Barlow rovněž přihlásil k myšlenkám Thomase Jeffersona, Johna Stuarta Milla, Jamese Madisona, Alexis de Tocquevilla a Louise Brandeise a k ideálu státem neomezené osobní svobody. Vzhledem k jejímu častému citování a širokému přijetí internetovou veřejností ji nelze považovat za pouhé vyjádření názoru jejího autora, nýbrž za skutečnou projekci ideálů a hodnot, které provázely vznik kyberprostoru a které vycházely z představ jeho tehdejších uživatelů.

Barlowův libertariánský[21] přístup k povaze kyberprostoru a dosahu státní moci však plně nezohledňuje skutečnost, že kyberprostor není světem svébytným, neodvozeným ani výhradním. Každý uživatel (či přeneseně obyvatel) kyberprostoru má ekvivalent v podobě hmotného člověka ve světě reálném. Stejně tak dopady jednání v kyberprostoru nebývají výhradně v rovině virtuální, ale mohou se výrazným způsobem projevit i ve světě reálném.

Na stranu druhou je třeba souhlasit s Barlowem, že vzhledem k decentralizovanosti internetu, praktické bezvýznamnosti hranic a s tím související obtížně určitelné aplikovatelnosti právních řádů jednotlivých států na různá jednání v rámci kyberprostoru lze hodnotit důslednou aplikaci státní moci v kyberprostoru za velmi obtížně uskutečnitelnou. Kyberprostor jako přirozeně se vyvíjející ekosystém založený na rovnosti jeho uživatelů a neexistenci centrálních regulačních prostředků se přesto projevil jako vysoce efektivní model informačního a komunikačního systému. Dle Polčáka se komplexní systémy i bez existence centrální autority

[19] BARLOW, John Perry. *A Declaration of the Independence of Cyberspace* [online]. [cit. 2021-5-30]. Dostupné z: https://www.eff.org/cyberspace-independence

[20] *Teorie společenské smlouvy* je koncept politické filosofie, kdy je existence veřejných mocenských a právních vztahů umožněna implicitní dohodou všech členů společnosti. Zdroj: *Společenská smlouva*. Wikipedia [online]. [cit. 2021-5-30]. Dostupné z: https://cs.wikipedia.org/wiki/ Spole%C4%8Densk%C3%A1_smlouva

[21] *Libertarianismus* je politická ideologie založená na idee bezstátní společnosti nebo společnosti s minimálním státem, přičemž za nejdůležitější hodnotu je považována co nejširší svoboda jednotlivce.

mohou bránit entropii[22] a chaosu autonomními autoregulačními mechanismy, které nepocházejí z žádné předem určené autority s normativní mocí, ale vznikající svévolně v důsledku dynamického vývoje systému ze vzájemných vztahů mezi jednotlivými subjekty. Prototypem takto popsaného decentralizovaného systému je právě internet, respektive kyberprostor jako celek. Výsledná kvalita organizovanosti takovéhoto systému pak nemusí odpovídat součtu přínosu jednotlivých prvků systému, nýbrž je modifikována jeho komplexitou. Polčák tento jev přirovnává k organizaci mraveniště. Jednotlivé mravence lze jen těžko označit za tvory s danou představou o uspořádanosti jejich společnosti, komplexita tohoto systému však zajišťuje efektivitu mnohonásobně přesahující fyzické i intelektuální možnosti všech jednotlivých mravenců v jejich vzájemném součtu.[23] Podobně hovoří i Hayek ve své *teorii rozptýlených informací*, která je ekonomickou teorií obhajující volný trh proti centrálnímu plánování, kdy dle této teorie soubor veškerých informací v rámci společnosti bude vždy rozptýlen mezi její jednotlivé prvky, přičemž žádný prvek systému, ani jeho centrální autorita, nikdy nemůže pojmout veškeré informace.[24]

Kyberprostoru tak nelze upřít schopnost autoregulace a existenci hodnotového rámce, na základě které jsou veškeré lidské společnosti založené. V kontextu předmětu této práce a vzhledem k aktuálnosti hrozeb spojených s kyberprostorem však dle mého názoru nelze na vymáhání práva v kyberprostoru rezignovat. Stále více se projevuje neoddělitelnost kybernetického a reálného světa, přičemž se ideály neomezené svobody a vzájemné tolerance bez byť minimalizované přítomnosti státní moci v prostředí internetu zejména v posledních několika letech zdají jako skutečnosti vzdálená utopie. Bez možnosti stíhat trestné činy učiněné v kontextu moderních komunikačních technologií orgány jednotlivých států při aplikaci norem trestního práva si lze jen těžko představit efektivní boj s nejrůznějšími kybernetickými hrozbami. I přes autoregulační schopnosti kyberprostoru v současné době neexistuje jiná možnost efektivního a rychlého potrestání pachatelů a odčinění způsobených škod, než prostřednictvím zásahu represivních orgánů státu, a to právě z důvodu neexistence jakékoliv jiné formy centrální autority, která by byla zmocněna k zásahu do práv a ke stanovení povinností jednotlivým subjektům v rámci kyberprostoru. Ačkoliv Barlow ve své deklaraci zmiňuje, že nelze použít právní koncepty založené na hmotě, jelikož v kyberprostoru žádná hmota neexistuje, nelze přehlížet situace, kdy v důsledku

[22] *Entropie* by se dala zjednodušeně označit za míru neuspořádanosti systému. Podle Polčáka je *informace* opakem entropie, je tedy mírou uspořádanosti systému.
[23] POLČÁK. Radim. *Autoritativní regulace kyberprostoru a legitimita trestního práva*. 2008. op. cit. s. 12 – 25.
[24] HAYEK, Friedrich August von. *Osudná domýšlivost: omyly socialismu*. Praha: Sociologické nakladatelství, 1995. ISBN 80-858-5005-2.

kriminálního jednání na internetu dojde ke škodlivému účinku například na zcela hmotném těle člověka. V tomto kontextu nelze nezmínit první případ zdokumentovaného lidského úmrtí, ke kterému mělo dojít v důsledku ransomware útoku na nemocnici v Německu v roce 2020.[25]

1.2 Kybernetická kriminalita

Problém s různorodým chápáním či s nejednotným označováním nalézáme rovněž při vymezení pojmu **kybernetická kriminalita**. Dle Koloucha je tato terminologická nejednotnost do značné míry zaviněná interdisciplinárností přístupu k řešení dané problematiky.[26] Kybernetická kriminalita je zkoumána z pohledu bezpečnostní analytiky, programování, práva, sociologie, kriminologie a dalších věd a odvětví.

Jako nejjednoduší definice kybernetické kriminality by se mohla jevit v návaznosti na výše uvedené ta, která říká, že kybernetická kriminalita je kriminalitou v kyberprostoru.[27] V tomto ohledu však nelze kybernetickou kriminalitu zaměňovat s pojmy počítačová kriminalita či internetová kriminalita, jelikož, jak již bylo uvedeno výše, kyberprostor není tvořen pouze sítěmi mezi počítači, ale rovněž mezi jinými zařízeními[28], a to i v rámci jiných sítí, než těch, které tvoří internet. Nelze však tvrdit ani to, že by počítačová kriminalita byla podmnožinou kybernetické kriminality. Útok na data uložená v počítači nepřipojeném k internetu ani jiné síti (například prostřednictvím zapojení infikovaného datového nosiče) lze jistě označit za projev počítačové kriminality, nejednalo by se však již o kriminalitu kybernetickou ve smyslu výše uvedené definice, jelikož by se takový útok neodehrával v kyberprostoru.

V odborné literatuře české i zahraniční však převažuje synonymní chápání těchto pojmů s tím, že vývojově starší pojem počítačová kriminalita je pojmem kybernetická kriminalita stále více nahrazován. Důvodem může být dle Koloucha právě i již zmiňovaný vývoj, kdy je funkcionalita zařízení nazývaného *osobním počítačem*[29] postupně nahrazována jinými technickými zařízeními, které nejsou v obecné řeči nazývány počítači.[30]

---

[25] ZOULOVÁ, Lenka. *Úmrtí kvůli hackerskému útoku? Byla to jen otázka času, míní bezpečnostní expert*. Novinky.cz [online]. [cit. 2021-5-30]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/umrti-kvuli-hackerskemu-utoku-byla-to-jen-otazka-casu-mini-bezpecnostni-expert-40337662
[26] KOLOUCH, Jan. *CyberCrime*. 2016. op. cit. s. 31.
[27] KRUPIČKA, Jiří. *Trestněprávní a kriminologické aspekty internetové kriminality*. 2012. op. cit. s. 13.
[28] Což je z hlediska předmětu této práce zásadní skutečnost, zejména s ohledem na stále častější ransomware útoky na „chytrá“ zařízení.
[29] Anglicky „personal computer“ – „PC“.
[30] KOLOUCH, Jan. *CyberCrime*. 2016. op. cit. s. 32.

Úmluva Rady Evropy o kybernetické kriminalitě[31] nepřináší konkrétní definici pojmu kybernetická kriminalita, napomáhá nám však s identifikací toho, co všechno lze pod tento pojem zařadit. Dle Budapešťské úmluvy rozlišujeme tyto kategorie kybernetických trestných činů:

- Trestné činy proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů;
- Trestné činy související s počítačem;
- Trestné činy související s obsahem;
- Trestné činy týkající se porušení autorského práva a práv souvisejících s právem autorským.

Kriminálními jevy, které spadají do kategorie **trestných činů proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů**, budou především nejrůznější typy neoprávněných průniků do počítačových systémů, neoprávněná změna a zničení dat uložených v počítačových systémech, šíření malware[32], DoS útoky[33], tvorba exploitů[34] a jiných metod sloužících k prolomení bezpečnostních opatření počítačových systémů. Právě do této kategorie spadá i šíření ransomware, které je předmětem této práce.

Kategorie **trestných činů souvisejících s počítačem** zahrnuje především padělání počítačových dat a počítačový podvod, které výslovně uvádí Úmluva o kybernetické kriminalitě. Gřivna tuto kategorii oproti Úmluvě o kybernetické kriminalitě rozšiřuje a označuje za „tradiční kriminalitu v novém kabátě“.[35]

Mezi **trestné činy související s obsahem** řadíme v první řadě šíření a jiné nakládání s dětskou pornografií, které zmiňuje i samotná Úmluva o kybernetické kriminalitě. Dále je možné pod tuto kategorii podřadit nejrůznější projevy násilí v kyberprostoru, jako je šíření

[31] ETS No.185 – Úmluva Rady Evropy č. 185 ze dne 23. 11. 2001 o kybernetické kriminalitě, rovněž označovaná jako Budapešťská úmluva.
[32] Tímto tématem se budu podrobně zabývat v následující kapitole.
[33] Zkratka pojmu *Denial of Service*, což v překladu z angličtiny znamená *odepření služby*. Principem DoS útoku je znepřístupnění cílové internetové stránky nebo služby jiným uživatelům, a to za pomoci velkého množství požadavků, které st zahltí, či využitím technické chyby takové služby. Poddtypem DoS útoku je tzv. *DDoS* útok (z angličtiny „*Distributed Denial of Service*“, lze přeložit jako „*distribuované odepření služby*“). Takový útok spočívá v přehlcení kapacity napadené služby či internetové stránky požadavky mnoha počítačů najednou, přičemž síť útočících počítačů je distribuovaná, počítače jsou tedy rozmístěné po celém světě.
[34] *Exploit* (angl.) lze přeložit jako *zneužití, využití*. V informatice se tento pojem používá pro vytvoření sekvence nebo programu na základě předem nezamýšlené chyby v programování. Zdroj: *Exploit*. Wikipedia [online]. [cit. 2021-5-30]. Dostupné z: https://cs.wikipedia.org/wiki/Exploit
[35] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ, Ivana. a kol. *Kriminologie. 5. aktualizované vydání*. 2019. op. cit. s. 393.

extremistického obsahu a kyberšikana, ale také šíření hoaxů[36] a spamu[37].[38] Aktuálním problémem je rovněž tzv. kybergrooming, který spočívá v psychologickém nátlaku na oběť činěný se sexuálním záměrem prostřednictvím kyberprostoru. Téma kybergroomingu vůči nezletilým dívkám v České republice veřejnosti přiblížil dokumentární film Víta Klusáka a Barbory Chalupové *V síti* (2020).

Trestné činy týkající se porušení autorského práva a práv souvisejících s právem autorským pak zahrnují veškeré formy porušování práv duševního vlastnictví v kyberprostoru. Tato jednání lze označit souhrnným pojmem *internetové pirátství*.

Kyberkriminalitu lze dále rozdělit na tradiční kriminalitu, která je prostřednictvím kyberprostoru a ICT technologií pouze usnadněna či urychlena, a takovou kriminalitu, která by bez ICT technologií byla nemyslitelná, jako je právě šíření malware.[39]

Ve své práci budu používat podobně jako většina autorů pouze pojem kybernetická kriminalita bez dalšího rozlišování mezi počítačovou kriminalitou, kybernetickou kriminalitou a internetovou kriminalitou, a to v širším smyslu zahrnujícím i tyto kategorie, ač jsem si vědom jisté nepřesnosti takto zavedeného pojmu.[40] Z hlediska předmětu této práce však nepovažuji rozlišování mezi těmito pojmy za účelné.

1.3 Malware

S kybernetickou kriminalitou je nedílně spojena problematika škodlivých kódů, tzv. malware. Tento pojem vznikl spojením dvou anglických výrazů, *malicious* (v překladu zlomyslný, zlovolný, škodlivý) a *software.*[41] Ačkoliv do českého jazyka se zpravidla slovo

[36] *Hoax* je klamavá zpráva. Prostřednictvím sítí komunikačních technologií se šíří zpravidla ve formě tzv. řetězových e-mailů.
[37] *Spam* je souhrnné označení pro nevyžádanou poštu. Původ slova spam je z obchodního pojmenování tradiční americké konzervy, nový význam toto slovo získalo díky skeči britské komediální skupiny Monty Python.
[38] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ, Ivana a kol. *Kriminologi. 5. aktualizované vydání*. 2019. op. cit. s. 398 - 400.
[39] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ, Ivana a kol. *Kriminologie. 5. aktualizované vydání*. 2019. op. cit. s. 393.
[40] Blíže k vymezení jednotlivých kategorií viz: KRUPIČKA, Jiří. *Trestněprávní a kriminologické aspekty internetové kriminality*. 2012. op. cit. s. 10 – 13.
[41] Programové vybavení počítače.

malware překládá právě jako škodlivý software či škodlivý kód, mezi malware bývá zpravidla řazen i takový software, který uživateli přímo neškodí, pouze jej obtěžuje.[42]

Kybernetické útoky prostřednictvím malware jsou činěny nejčastěji za účelem prolomení ochrany zařízení a získání přístupu k datům uživatele a jejich následnému zneužití či poškození. Rovněž se lze setkat s takovým typem malware, jehož cílem je získat kontrolu nad napadeným zařízením.[43] Na základě dělení kybernetické kriminality podle Budapešťské úmluvy bychom je tak řadili mezi trestné činy proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů.

Malware patří mezi kybernetickou kriminalitu, která by neexistovala bez ICT technologií, dle Walla lze takovou kriminalitu přiblížit úslovím *„new wine no bottles“*.[44] Malware je do jisté míry spjat s hackerskou kulturou a jeho historie sahá až k samotným kořenům internetu.[45] Z pohledu široké laické veřejnosti bývá malware (v běžné řeči je často nepřesně označován českým výrazem *počítačové viry*) společně s hackingem často vnímán jako téma exotické, tajemné a vzrušující, což je zřejmě dáno kombinací jeho těžké uchopitelnosti pro osoby neznalé programování a kybernetické bezpečnosti a častou romantizací v dílech populární kultury. Malware, zvláště pak některé jeho kategorie, jako právě ransomware, je však odbornou veřejností považován za jednu z aktuálně nejpalčivějších bezpečnostních hrozeb.[46]

Malware můžeme dělit podle mnoha kritérií. Nejčastěji se setkáváme s dělením podle funkcionality a charakteristických vlastností daného programu. Vzhledem k obrovskému počtu

---

[42] Příkladem může být tzv. *adware* (ang. *ad* – reklama; *software*), tedy software zobrazující uživateli vyskakovací okna s nevyžádanou reklamou. K tomuto blíže např.: *Co je to adware?* Avast [online]. [cit. 2021-7-21]. Dostupné z: https://www.avast.com/cs-cz/c-adware

[43] Zpravidla za účelem zapojení napadeného zařízení do tzv. *botnetu*, tedy sítě počítačů ovládaných z jednoho centra často bez vědomí jednotlivých uživatelů. Počítači zapojenému do botnetu se přezdívá *zombie*. Botnety mohou být zneužívány ke kybernetickým útokům typu DDoS.

[44] V překladu z angličtiny *„nové víno bez lahví“*. Wall toto úsloví používá v kontrastu s původním rčením *„new wines in old bottles“* tedy doslova *„nová vína ve starých lahvích“*, kterým označuje tu kybernetickou kriminalitu, která může být páchána i mimo kontext ICT technologií. Jako příklad lze uvést porušování autorských práv či podvod. WALL, David. *Cybercrimes: New Wine, No Bottles?* 1999. In: DAVIES, Pamela, FRANCIS, Peter, JUPP, Victor, *Invisible Crimes*. London: Palgrave Macmillan. 1999. ISBN: 978-1-349-27641-7. Dostupné také z: DOI: 10.1007/978-1-349-27641-7. s. 105-139.

[45] Prvním programem, který je možné označit za malware, byl počítačový červ s názvem *Creeper*, kterým byla infikována počítačová síť ARPANET, která je považována za přímého předchůdce dnešního internetu, a to již v roce 1971. *Creeper* však nebyl škodlivým programem, nakažené počítače pouze zobrazily hlášku *"I'm the creeper: catch me if you can"* (v překladu *„Já jsem creeper, chyť mě, jestli to dokážeš“*). Zdroj: MELTZER, Tom, PHILLIPS, Sarah. *From the first email to the first YouTube video: a definitive internet history*. The Guardian [online]. [cit. 2021-5-30]. Dostupné z: https://www.theguardian.com/technology/2009/oct/23/internet-history

[46] Národní úřad pro kybernetickou a informační bezpečnost ČR. *Analýza hrozby ransomware*. [cit. 2021-5-30] Dostupné z: https://nukib.cz/download/publikace/analyzy/Analyza_hrozby_ ransomware.pdf

variant malware a snaze útočníků tvořit stále odolnější a variabilnější kódy však konkrétní malware může svými charakteristikami odpovídat i několika z uvedených skupin.[47]

Počítačový vir je typem malware, jehož charakteristickou vlastností je multiplikace škodlivého kódu do dalších souborů v počítači. Životní cyklus počítačového viru se podobá životnímu cyklu biologického viru v těle živého organismu, přičemž počítačový virus využívá jednotlivé soubory obdobně jako skutečný virus buňky svého hostitele. Z hlediska šíření na jiná zařízení jsou však počítačové viry závislé na prostředníkovi, nejčastěji na samotném uživateli.

Počítačový červ se oproti viru vyznačuje schopností šířit se mezi zařízeními samostatně, bez prostředníka. Může se šířit prostřednictvím počítačových sítí za využití zranitelností počítačových systémů.

Trojský kůň je takovým typem malware, který se vydává za pro uživatele užitečný software či jiný obsah. Při své distribuci tak tento typ malware spoléhá na aktivitu uživatele, který si není vědom pravé podstaty distribuovaného obsahu. Svým pojmenováním odkazuje na slavný příběh z řecké mytologie o dobytí Tróje za použití *danajského daru*, dřevěného koně s ukrytými řeckými vojáky.

Spyware je software určený ke sledování aktivity uživatele bez jeho vědomí. Jeho název vznikl spojením anglických slov *spy* (v překladu špeh, špion) a *software*. Tento druh malware se může vyznačovat sledováním a ukládáním stisku kláves na klávesnici, taková činnost bývá zacílena na sběr přihlašovacích údajů a hesel uživatele, které jsou následně odesílány útočníkovi. Takový typ spyware pak funguje jako tzv. **keylogger**[48].

Adware je často neškodným programem, jehož účelem je zobrazování reklamy uživateli. Může se projevovat například zobrazováním vyskakovacích oken nebo změnou domovské stránky v prohlížeči. Do zařízení uživatele se zpravidla dostane společně s jiným bezplatným softwarem. Jeho škodlivost spočívá v obtěžování uživatele, ve vyskakovacích oknech navíc může zobrazovat pornografický či jiný nežádoucí obsah. Nebezpečným se adware stává ve chvíli, kdy kombinuje prvky jiných typů škodlivých kódů, nejčastěji spyware. Může pak docházet ke sledování činnosti uživatele za účelem snadnějšího zacílení reklamy či dokonce k odcizení osobních dat včetně přihlašovacích jmen a hesel. Adware se však může vyskytovat i jako zcela legální funkcionalita

[47] BRONIEK, David. *Analýza malware*. Ostrava. 2019. Diplomová práce. Vysoká škola báňská – Technická univerzita Ostrava, Fakulta elektrotechniky a informatiky. Vedoucí práce prof. Ing. Ivan Zelínka, Ph.D., s. 21.
[48] Z angličtiny *key* – v překladu klíč a *logger* – záznamník. Kromě softwarového keyloggeru existují také hardwarové zařízení fungující jako keyloggery, mohou mít například podobu zařízení zapojeném mezi klávesnicí a počítačem.

komerčního programu, kdy výrobce inzeruje v rámci bezplatné verze plnou verzi používaného software.

Rootkity jsou sady nástrojů, jejichž účelem je skrývání přítomnosti malwaru v napadeném zařízení. Rootkity jsou obtížně odhalitelné i za použití moderních antivirových programů, mohou tak v napadeném zařízení působit dlouhodobě.

O povaze dalšího typu malware, **ransomware**, jehož trestněprávní a kriminologická analýza je předmětem této práce, pojednává následující kapitola.

1.4 Ransomware

Jako ransomware označujeme takový typ škodlivého software, který využívá znepřístupnění či omezení napadeného systému a dat v něm uložených k vydírání uživatele. K tomu používá často prostředky symetrické či asymetrické kryptografie[49], kdy po infikaci systému dojde k zašifrování dat uživatele a k zobrazení výzvy útočníka, aby napadený uživatel převedl na útočníkův účet požadovaný finanční obnos (dnes již téměř výhradně v podobě kryptoměn[50]) pod příslibem následného dešifrování znepřístupněných souborů. Uživateli je zpravidla vyměřen časový limit pro provedení platby, po jehož vypršení má dojít ke smazání soukromého klíče, tedy k nevratnému znepřístupnění zašifrovaných dat. Odtud označení ransomware, kdy *ransom* znamená v překladu z angličtiny *výpalné* či *výkupné*. Existuje však celá řada dalších rozličných způsobů, kterými útočníci působí na uživatele ve snaze získat finanční prospěch, od jednoduchého znepřístupnění ovládacích prvků napadeného systému až po vydávání se za orgán veřejné moci.

Cílem ransomwarového útoku mohou být jak běžní uživatelé, kteří bývají z důvodu potencionálně nízké rentability cílem plošných a méně sofistikovaných útoků, tak obchodní společnosti a podniky, u kterých bývá zpravidla vyšší motivace zaplatit výkupné z důvodu možnosti vyšších finančních ztrát a z obavy ze ztráty důvěry zákazníků[51] či ze zveřejnění

---

[49] *Symetrické kryptografie* je kryptografickou metodou, kdy je pro zašifrování i dešifrování použit stejný klíč. V případě *asymetrická kryptografie* je pro dešifrování dat používán odlišný klíč (soukromý klíč) než byl použit pro jeho zašifrování (veřejný klíč). Při použití moderních metod asymetrické kryptografie je zpětné dešifrování dat bez znalosti soukromého klíče prakticky nemožné, nevýhodou je však pomalé šifrování dat. Obě metody mohou být kombinovány, poté hovoříme o tzv. *hybridní kryptografii*.

[50] Kryptoměny jsou decentralizované digitální peníze založené na technologii blockchainu. Blockchain je otevřená distribuovaná globální databáze fungující jako účetní kniha. Ochrana finančních prostředků na jednotlivých účtech je zajištěna prostřednictvím kryptografických metod. Historicky první a nejrozšířenější kryptoměnou je Bitcoin.

[51] NÚKIB. *Analýza hrozby ransomware*. Dostupné z: https://nukib.cz/download/publikace/analyzy/Analyza_hrozby_ransomware.pdf. str. 2.

obchodního tajemství a know-how. Stále častěji bývají cílem ransomware útoků veřejné subjekty, jako jsou nemocnice a územní samosprávy, dále pak orgány státní správy či poskytovatelé dopravních služeb (letiště, nádraží a přístavy).[52]

K infikaci počítače nebo jiného zařízení ransomware může dojít prostřednictvím e-mailové zprávy se škodlivou přílohou nebo s odkazem na webové stránky obsahující malware. Tuto metodu útoku označujeme jako **malspam**,[53] výraz vznikl kombinací anglických slov *malware* a *spam*. Malspam využívá metody *sociálního inženýrství*[54], kdy se útočník svým psychologickým působením snaží přimět uživatele k otevření přílohy nebo ke kliknutí na vložený odkaz. Nebezpečný e-mail se může maskovat za oznámení o výhře značné částky, za zprávu o úmrtí vzdáleného příbuzného v zahraničí, který uživateli zanechal značné jmění, či za zprávu Nigerijského prince nabízející uživateli pohádkově výhodnou transakci.[55] Tento typ sociálního inženýrství bývá označován jako **phishing**[56] a kromě šíření malwarových hrozeb[57] bývá často užíván pro získání citlivých informací oběti, jako jsou čísla kreditních karet, přihlašovací jména a hesla, či mohou uživatele dovést k dobrovolnému odeslání finančního obnosu na útočníkův účet. Tyto typy nepříliš rafinovaných útoků zpravidla nepředstavují velkou kybernetickou hrozbu, jelikož jsou snadno rozpoznatelné svým špatným nebo neúplným překladem a mnohdy až absurdním obsahem. Kromě uvedených dnes již i mezi laickou veřejností dobře známých metod se lze však setkat i s vyspělými phishingovými metodami, kdy například útočník předstírá, že je zaměstnancem banky uživatele, přičemž veškeré grafické prvky e-mailu jsou shodné s grafickými prvky banky.[58] Rovněž lze zmínit velmi vyspělou variantu phishingu, tzv. **spear phishing**[59], který

---

[52] NÚKIB. *Analýza hrozby ransomware*. Dostupné z: https://nukib.cz/download/publikace/analyzy/Analyza_hrozby_ransomware.pdf. str. 2.

[53] *Ransomware - What is it & how to remove it*? Malwarebytes [online]. [cit. 2021-5-14]. Dostupné z: https://www.malwarebytes.com/ransomware/

[54] Sociální inženýrství v kontextu kybernetické bezpečnosti je způsob prolamování bezpečnostních opatření za pomoci psychologického působení na člověka. Zjednodušeně lze tuto metodu charakterizovat známým úslovím, že nejslabším článkem každého bezpečnostního systému je uživatel.

[55] *SCAM419* [online]. [cit. 2021-5-14]. Dostupné z: https://www.hoax.cz/scam419/

[56] Pojem phishing vznikl z anglického slova *fishing* (rybaření). *Ph* nahrazující *f* zřejmě odkazuje na starší slangový pojem *phreak* (*phone* – telefon, *freak* – blázen, nadšenec), kterým se označovali lidé znalí technické stránky telekomunikačních služeb, kteří své znalosti zneužívali k vyhýbání se placení za telefonní hovory a k dalším nelegálním činnostem. V češtině se někdy objevuje tvar *rhybaření*.

[57] Podle společnosti Avast v roce 2016 ransomware obsahovalo 93 % phishingových e-mailů. Zdroj*: Ransomware: A billion-dollar problem*. Blog.avast [online]. [cit. 2021-5-14]. Dostupné z: https://blog.avast.com/ransomware-a-billion-dollar-problem

[58] *Phishingové útoky už dávno nejsou jen hloupé*. Computerworld [online]. [cit. 2021-5-15]. Dostupné z: https://computerworld.cz/securityworld/phishingove-utoky-uz-davno-nejsou-jen-hloupe-50888.

[59] *Spear fishing* v překladu znamená rybaření oštěpem. S touto aktivitou má kybernetický *spear phishing* společnou charakteristiku v zaměření na konkrétní cíl.

zpravidla cílí na významné společnosti a orgány veřejné moci, kdy jsou metody sociálního inženýrství postavené na dlouhodobé špionáži zacíleného subjektu.

Infikovaný e-mail kromě phishingových metod může využívat i dalších metod sociálního inženýrství, jako je například **clickbait**[60], kdy je uživatel ke kliknutí na odkaz nebo k otevření přílohy přiměn slibem lákavého obsahu (často pornografického) nebo šokující zprávou.

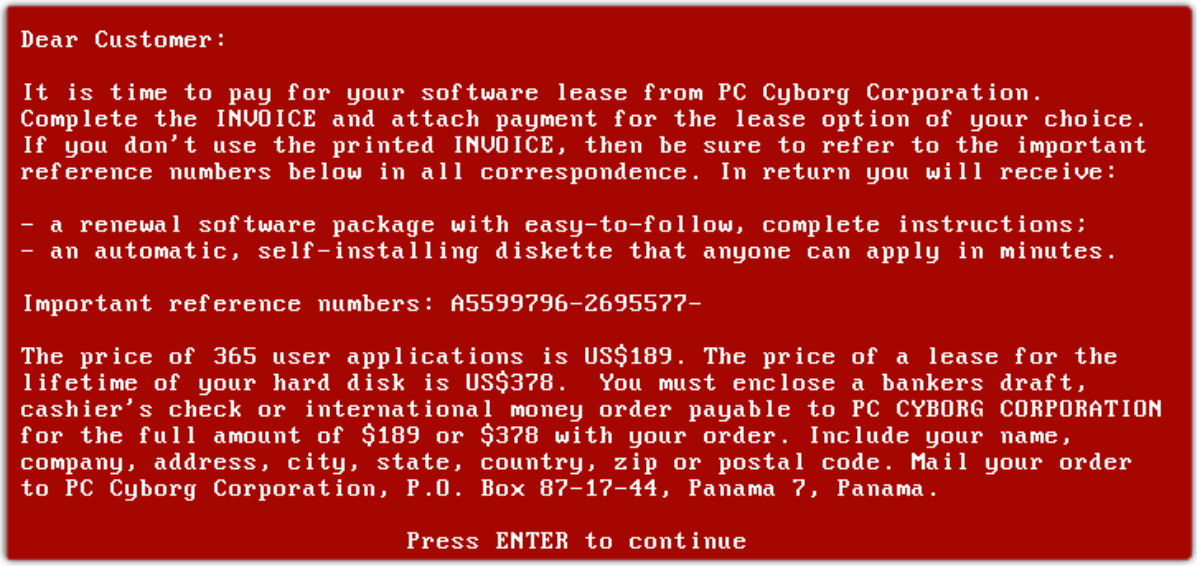
Ačkoliv se setkáváme s čím dál vyspělejšími metodami phishingu a jiných typů sociálního inženýrství, u výše uvedených vektorů útoku je vždy nutná určitá míra součinnosti uživatele a takový typ útoku je tak zpravidla při dobré informovanosti uživatele odvratitelný. Z tohoto hlediska se tak jako větší hrozba jeví druhá častá metoda šíření ransomware, která nabývá na intenzitě zvláště v několika posledních letech.[61] Jedná se o tzv. **malvertising**. Tato metoda zneužívá online reklamu k šíření škodlivého kódu, a to i bez nutnosti bližší interakce uživatele s takovou reklamou. Odtud i označení pocházející ze spojení slov *malicious* a *advertising* (český překlad *propagace*, *reklama*). Mohlo by se sice zdát, že se jedná o problém převážně méně důvěryhodné části internetu, množí se však případy malvertisingu na známých a velmi frekventovaných webech[62].

1.4.1 Historie a dosavadní vývoj ransomware

Za první ransomware bývá označován malware *AIDS Trojan*[63] vytvořený roku 1989 evolučním biologem Dr. Josephem Poppem. Šíření tohoto škodlivého kódu probíhalo prostřednictvím rozesílání disket s dotazníkem o onemocnění AIDS. Dr. Popp diskety distribuoval vytipovaným subjektům, mezi jinými i účastníkům konference o viru HIV pořádané Světovou zdravotnickou organizací. Po instalaci distribuovaného softwaru začal malware počítat každé spuštění systému a jakmile dosáhl čísla 90, zašifroval názvy souborů včetně přípon na disku C:, čímž je učinil pro uživatele nespustitelnými, a zobrazil obrazovku s požadavkem na zaplacení poplatku za užívání softwaru. Platbu měli uživatelé provést zasláním platební směnky, šeku nebo poštovní poukázky na P. O. Box v Panamě.

---

[60] Složenina anglických slov *click* (kliknutí) a *bait* (návnada).
[61] *Truth in malvertising: How to beat bad ads*. Malwarebytes [online]. [cit. 2021-5-15]. Dostupné z: https://blog.malwarebytes.com/101/2016/06/truth-in-malvertising-how-to-beat-bad-ads/
[62] Příkladem může být malvertisingový útok nesoucí ransomware na uživatele služby Yahoo! v roce 2015. Zdroj: *Yahoo users hit by 'malvertising' campaign*. The Guardian [online]. [cit. 2021-5-15]. Dostupné z: https://www.theguardian.com/technology/2015/aug/05/yahoo-users-malvertising-campaign-malware
[63] Jinak označovaný také jako *PC Cyborg Trojan*.



Obrázek 1 – AIDS Trojan[64]

Význam tohoto škodlivého kódu pro pozdější generace ransomware lze spatřovat primárně v samotné idee, že malware je možné zneužít jako prostředek pro vydírání oběti a generování určitého zisku, nikoliv pouze jako způsob, jak zničit data v napadeném zařízení či jak zkomplikovat práci s počítačem méně zkušeným uživatelům, jak tomu bylo doposud. Jak uvedli Young a Yung, podstatnou novinkou bylo použití kryptografie nikoliv jako způsobu zabezpečení soukromí uživatele a jeho dat, nýbrž právě naopak, jako metody útoku proti uživateli a jeho datům.[65] Co se však technické vyspělosti malwaru a jeho rentability týče, nelze AIDS Trojan považovat za příliš úspěšný. Jim Bates, který provedl v roce 1990 analýzu tohoto malware[66] a následně vytvořil programy AIDSOUT a AIDSCLEAR k jeho odstranění a k dekryptování souborů, označil programování AIDS Trojanu i přes vynalézavost a prohnanost jeho myšlenky za nepořádné[67]. Young a Yung za jeho největší technickou slabinu považovali použití symetrického šifrování, tedy takové šifrovací metody, kde je k šifrování i dešifrování dat použit stejný klíč. Ve své práci předpověděli budoucí vývoj tohoto typu kybernetického útoku směrem k asymetrickému šifrování.[68] Za netechnické důvody malé finanční výnosnosti AIDS Trojanu lze považovat

[64] Zdroj: https://en.wikipedia.org/wiki/AIDS_(Trojan_horse)#/media/File:AIDS_DOS_Trojan.png.
[65] YUNG, Moti, YOUNG, Adam. *Cryptovirology: extortion-based security threats and countermeasures*. IEEE Symposium on Security and Privacy. Oakland: IEEE Comput. Soc. Press, 1996. ISBN 0-8186-7417-2. Dostupné z: doi:10.1109/SECPRI.1996.502676. st. 129.
[66] BATES, Jim. Technical analysis: *Trojan Horse: AIDS Information Introductory Diskette Version 2.0.* Virus Bulletin. Oxon: Virus Bulletin, 1990(January), ISSN 0956-9979. st. 3-6.
[67] V originále „untidy". Tamtéž.
[68] YUNG, Moti, YOUNG, Adam. *Cryptovirology: extortion-based security threats and countermeasures*. 1996. op. cit.

omezené možnosti jeho distribuce, malý počet uživatelů počítačů a špatné zacílení, ale i skutečnost, že zaplacení požadované částky nebylo zcela jednoduchým úkonem, nebylo dnešní terminologií „na pár kliků“, jak je tomu u moderních ransomwarů.

Až do roku 2005 nedošlo k žádnému dalšímu významnému šíření ransomware. V roce 2005 se začaly ve větší míře objevovat zástupci tzv. *scareware*[69]. Patřil mezi ně například *SpySheriff*, malware „strašící“ uživatele častým zobrazováním upozornění na přítomnost škodlivého spyware v počítači. Při zobrazení upozornění uživatele vyzývá k zakoupení programu.[70] Rovněž v témže roce došlo k rozšíření trojského koně s názvem *PGPCoder* nebo *GPCode* ruského původu. Šlo o šifrovací ransomware, který, stejně jako AIDS Trojan, používal pouze symetrické šifrování. Jeho prolomení tak nebylo příliš obtížné.

K prvnímu významnějšímu posunu v technologii ransomware došlo však až v roce 2006, kdy došlo k rozšíření prvního ransomwaru využívajícího asymetrické šifrování, konkrétně 1024bitového RSA algoritmu. Jednalo se o malware *Archievus*. Zajímavostí na tomto ransomware, kromě pokročilé metody šifrování za použití veřejného klíče, byla skutečnost, že šifroval pouze soubory uložené ve složce *Moje dokumenty*. Vzhledem ke skutečnosti, že většina uživatelů v té době veškeré důležité dokumenty ukládala právě do této složky a jejích podsložek, jeho škodlivým účinkům toto specifikum nezabránilo.[71]

V pozdějších letech docházelo k prvním výskytům nových typů ransomware, a to *locker ransomware*[72] a tzv. *policejních virů*. Policejní viry se staly rozšířenými i v České republice, první počeštěné verze patřící do této rodiny ransomware, které se začaly objevovat v roce 2012, však nedisponovaly příliš kvalitním českým překladem.[73]

Jedním z nejznámějších ransomware v historii se stal *CryptoLocker*, který se objevil v roce 2013 a šířil se až do poloviny roku 2014. K distribuci tohoto ransomware docházelo především prostřednictvím masivního botnetu s názvem *Gameover ZeuS*, který byl využíván k šíření škodlivého kódu přes webové stránky. Za vznikem botnetu stál ruský hacker Evgeniy Mikhailovich Bogachev a kromě šíření *CryptoLocker* ransomware byl zneužíván rovněž ke kybernetickým útokům na bankovní účty. Šíření prostřednictvím botnetu napomohlo masivnímu

---

[69] Tomuto typu škodlivého kódu se budu blíže věnovat v podkapitole 1.4.2.
[70] CSIRT.CZ. Historie a vývoj ransomwaru: všechno to začalo s AIDS. Lupa.cz [online]. [cit. 2021-5-15]. Dostupné z: https://www.lupa.cz/clanky/historie-a-vyvoj-ransomwaru-vsechno-to-zacalo-s-aids/
[71] *Historie ransomware hrozeb: jak to bylo, je a bude* [online]. [cit. 2021-5-18]. Dostupné z: https://cs.vpnmentor.com/blog/historie-ransomware-hrozeb-minulost-soucasnost-budoucnost/
[72] Za první locker ransomware bývá označován *WinLock Trojan*, který se rozšířil v roce 2011.
[73] *Policie ČR vás sleduje!* Viry.cz [online]. [cit. 2021-5-18]. Dostupné z: https://viry.cz/policie-cr-vas-sleduje/

rozšíření ransomware po celém světě. *CryptoLocker* ransomware používal pokročilou metodu 2048bitového RSA šifrování za využití sítě *Tor*[74]. Za poražením tohoto ransomware stála spolupráce policejních orgánů, bezpečnostních agentur, akademických pracovišť a společností zabývajících se kybernetickou bezpečností v rámci operace s názvem *Operation Tovar*[75], které se povedlo dočasně narušit *Gameover ZeuS* botnet a získat přístup k databázi soukromých klíčů užitých *CryptoLockerem* k zašifrování dat uživatelů. Úspěch operace Tovar nám ukazuje, že k boji proti globálně se šířícím kybernetickým hrozbám je zapotřebí spolupráce mezinárodní se zapojením jak veřejného, tak i soukromého sektoru. V roce 2015 se poprvé objevil obchodní model prodeje ransomware „na klíč" označovaný jako *ransomware-as-a-sevice*[76].

Do dějin ransomware se výrazně zapsal rok 2017, kdy došlo ke globálnímu masivnímu kybernetickému útoku ransomwarem *WannaCry*. V pátek 12. května 2017, první den útoku, bylo infikováno nejméně 75 000 počítačů v 99 zemích po celém světě.[77] O několik dní později bylo napadených zařízení čtvrt milionu.[78] *WannaCry* funguje na principu počítačového červa, který se šíří za využití bezpečnostní chyby v systému Windows, nevyžaduje tak vůbec žádnou aktivitu uživatele. Tato zranitelnost systémů Windows přitom byla již několik let známa americké zpravodajské službě NSA, která ji využívala ke sledování uživatelů jako tzv. *EternalBlue exploit*[79]. V dubnu roku 2017 došlo k úniku a zveřejnění tohoto exploitu, následně byla společností Microsoft vydána záplata odstraňující tuto zranitelnost. I přesto následný útok *WannaCry* využívající tento exploit zasáhl celosvětově obrovské množství počítačů se systémem bez potřebné aktualizace či počítače, které ještě stále používaly systém Windows XP. Mezi napadenými zařízeními byly i nemocnice britské zdravotní služby NHS, zařízení dopravní infrastruktury, servery významných společností a další.[80]

---

[74] *Tor* (název vznikl jako zkratka původního vojenského projektu s názvem *The Onion Router*) je bezplatným open-source softwarem a sítí umožňující uživatelům anonymní komunikaci, a to na základě šifrování a přesměrování dat v několika vrstvách. Zdroj: *Co je Tor?* Alza.cz [online]. [cit. 2021-5-21]. Dostupné z: https://www.alza.cz/co-je-tor

[75] Přehled zúčastněných orgánů a dalších subjektů lze nalézt zde: SOARE, Bianca. *Operation Tovar: What It Was and How A Key Botnet Was Eliminated*. Heimdal security [online]. [cit. 2021-5-21]. Dostupné z: https://heimdalsecurity.com/blog/operation-tovar/

[76] V překladu z angličtiny *ransomware jako služba*. Blíže bude toto téma rozebíráno v kapitole 1.4.3.

[77] *Cyber-attack: Europol says it was unprecedented in scale*. BBC [online]. [cit. 2021-5-18]. Dostupné z: https://www.bbc.com/news/world-europe-39907965

[78] *Historie ransomware hrozeb: jak to bylo, je a bude*. VpnMentor [online]. [cit. 2021-5-18]. Dostupné z: https://cs.vpnmentor.com/blog/historie-ransomware-hrozeb-minulost-soucasnost-budoucnost/

[79] BURDOVA, Carly. *What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?* Avast [online]. [cit. 2021-9-2]. Dostupné z: https://www.avast.com/c-eternalblue

[80] *Historie ransomware hrozeb: jak to bylo, je a bude*. VpnMentor [online]. op. cit.

Obrázek 2 – WannaCry ransom note[81]

I přes obrovskou úspěšnost v šíření podle dostupných informací *WannaCry* nepřinesl svým autorům velký finanční zisk.[82] Za útokem stála hackerská skupina *Lazarus*, podporovaná severokorejskou vládou.[83]

Ve stejné době došlo k masivnímu šíření ransomware *Petya*, který fungoval na principu totožného exploitu jako *WannaCry*. V roce 2017 proběhl rozsáhlý kybernetický útok se zaměřením na ukrajinské počítače, za kterým stála jeho varianta někdy označovaná jako *NotPetya*.[84]

---

[81] Zdroj: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#/media/File:Wana_Decrypt0r_screenshot.png
[82] MACFARLANE, Alec. *Why the massive cyberattack won't make the hackers rich*. CNN Business [online]. [cit. 2021-5-21]. Dostupné z: https://money.cnn.com/2017/05/17/technology/wannacry-ransomware-bitcoin-cyberattack/index.html
[83] JOHNSON, A. L. *WannaCry: Ransomware attacks show strong links to Lazarus group*. Broadcom [online]. [cit. 2021-5-21]. Dostupné z: https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=b2b00f1b-e553-47df-920d-f79281a80269&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
[84] NG, Alfred. *US: Russia's NotPetya the most destructive cyberattack ever*. CNet [online]. [cit. 2021-9-2]. Dostupné z: https://www.cnet.com/tech/services-and-software/uk-said-russia-is-behind-destructive-2017-cyberattack-in-ukraine/

Do povědomí české veřejnosti se ransomware útoky dostaly po infikaci systémů benešovské nemocnice a systémů společnosti OKD v prosinci 2019.[85]

1.4.2 Typy ransomware

Ačkoliv je ransomware vnímán jako jednotný ucelený fenomén, z hlediska způsobu útoku a technického zpracování mezi jeho jednotlivými variantami existují podstatné rozdíly. Jednotícím parametrem ransomware je především určitý způsob vydírání uživatele za účelem dosažení finančního zisku. Jak již bylo uvedeno výše, ransomware vydírá napadeného uživatele prostřednictvím omezení přístupu k zařízení nebo datům, zašifrováním dat, hrozbou zveřejnění dat nebo hrozbou sankce udělené orgány veřejné moci.

Šifrovací ransomware (nebo také *crypto ransomware*) při své aktivaci zašifruje data uživatele a za jejich odšifrování požaduje po uživateli výkupné, zpravidla ve formě platby prostřednictvím Bitcoinů. Moderní ransomware pro šifrování používají asymetrickou kryptografii, pro odšifrování souborů je tak zapotřebí znalost soukromého klíče. Pro zesílení psychologického nátlaku je zpravidla uživateli poskytnuta lhůta k provedení platby, po jejímž vypršení dojde ke smazání soukromého klíče a tedy k nenávratné ztrátě zašifrovaných dat. I při zaplacení požadované částky však neexistuje jistota, že k obnovení dat skutečně dojde. Jako příklady šifrovacích ransomware lze jmenovat *WannaCry*, *Petya*, *CryptoLocker* či *AIDS Trojan*.

Locker ransomware na rozdíl od šifrovacích ransomware nijak nepozměňuje data uživatele, pouze omezuje přístup uživatele k zařízení prostřednictvím překrytí obrazovky *ransom note*[86] oknem či blokací některých ovládacích prvků.[87] Příkladem tohoto typu škodlivého kódu je *WinLock*.

Doxware je takový typ ransomware, který uživateli vyhrožuje zveřejněním napadených dat. Tento typ škodlivého kódu se objevil až v posledních několika letech a zaměřuje se převážně na velké společnosti, u kterých existuje obava ze zveřejnění obchodního tajemství či know-how a je zde zvýšená ochota zaplatit požadované výkupné. Aktuálním příkladem doxware zaměřujícího se na velké společnosti jsou škodlivé kódy z rodiny *maze ransomware*[88].

---

[85] *Za útokem na benešovskou nemocnici byl ruský vir Ryuk*. ČT24 [online]. [cit. 2021-5-30]. Dostupné z: https://ct24.ceskatelevize.cz/regiony/stredocesky-kraj/3029729-za-utokem-na-benesovskou-nemocnici-byl-rusky-vir-ryuk

[86] V překladu z angličtiny *vyděračský vzkaz*.

[87] BRONIEK, David. *Analýza malware*. Ostrava. 2019. Diplomová práce. op. cit. s. 25.

[88] *What is maze ransomware? Definition and explanation*. Kaspersky [online]. [cit. 2021-5-21]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/what-is-maze-ransomware

Policejní virus využívá k vylákání finančních prostředků od uživatele vydáváním se za sdělení orgánu veřejné moci. Zpravidla dochází k omezení přístupu uživatele k systému nebo k jeho datům v kombinaci se zobrazením sdělení, že se uživatel dopustil protiprávního jednání a že případným právním následkům lze zabránit zasláním platby na účet útočníka. Tento typ ransomware není zpravidla z technického hlediska obtížně odstranitelný[89], jeho efektivita je zaručena primárně psychologickým působením na uživatele.

Obrázek 3 – Jedna z variant policejního viru[90]

Scareware se podstatně liší od ostatních typů ransomware v tom, že základní metodou vylákání finančního obnosu od uživatele napadeného systému není vydírání, ale decepce. Scareware uživateli při aktivaci zobrazí upozornění zpravidla o infikaci jeho zařízení určitým typem malware a nabízí řešení v podobě zakoupení fiktivního antivirového programu. Ve své podstatě tento škodlivý software nesplňuje základní definici ransomware, kterou jsem uvedl výše, jelikož zde chybí *ransom*, tedy výkupné, mezi ransomware však bývá tradičně řazen.[91]

---

[89] Řešení nabízí např. tento článek: BUCHTA, Martin. *Jak odstranit policejní vir?* ESET [online]. [cit. 2021-5-25]. Dostupné z: https://servis.eset.cz/knowledgebase/article/View/257/46/jak-odstranit-policejni-vir#.YK4FxagzaUk

[90] Zdroj: https://www.policie.cz/clanek/objevuje-se-vam-na-monitoru-podezrele-hlaseni.aspx

[91] Mezi ransomware tento typ útoku řadí i NÚKIB. Viz: NÚKIB. *Analýza hrozby ransomware*. Dostupné z: https://nukib.cz/download/publikace/analyzy/Analyza_hrozby_ ransomware.pdf

1.4.3 Ransomware-as-a-service

V předchozích letech došlo ve světě kyberkriminality k zásadnímu posunu od tvorby software svépomocí, komunitního sdílení a *open-source*[92] mentality ke komercializaci a kapitaliazaci kybernetického zločinu. Tento trend se projevil i ve tvorbě a šíření ransomware jako tzv. *ransomware-as-a-service (RaaS)*. Jedná se o obchodní model používaný vývojáři ransomware, kdy za jednorázový nebo měsíční poplatek nabízejí jimi vytvořený ransomware klientům. Tento model může zahrnovat kromě samotného kódu i plnou zákaznickou podporu, slevové balíčky i zákaznická fóra.[93] Již dnes je úroveň profesionalizace RaaS služeb na úrovni bežných softwarových služeb poskytovaných standardními společnostmi zaměřujícími se na tvorbu software řešení pro společnosti a veřejný sektor, přičemž se dá očekávat ještě větší profesionalizace a komercializace tohoto zločineckého odvětví.

RaaS umožnilo vstup do ransomware světa i těm útočníkům, kteří sami nedisponovali technickými dovednostmi potřebnými k vytvoření škodlivého kódu a k úspěšnému provedení kybernetického útoku. Podle některých bezpečnostních společností[94] k rozvoji RaaS přispělo vybudování nelegálních online tržišť v rámci tzv. *darknetu*[95], jako byl dnes již zrušený *DarkMarket*.

Podle studie Melanda, Bayoumy a Sindreho jsou však tvrzení o velké rozšířenosti RaaS na darknetu přehnaná.[96] Uvádí, že na základě několikaletého zkoumání na tržnicích darknetu odhalili, že jen malé procento nabízeného zboží a služeb bylo RaaS. Určitá část nabízeného softwaru označeného jako ransomware přitom byla falešná, nebo převáděla získané finanční prostředky na jiný účet, než na účet zákazníka RaaS. Autoři však současně uvedli, že součástí jejich výzkumu nebyla uzavřená fóra, komunity, které jsou dostupné pouze s pozvánkou, a neanglická fóra (dá se přitom předpokládat, že např. ruské tržnice budou svým obsahem významně odlišné od těch anglických). Zůstává tak otázkou, zda uvedený výzkum věrně reflektuje skutečné množství existujících RaaS služeb dostupných na darknetu.

---

[92] *Open-source software* (česky *software s otevřeným kódem*). Jedná se o počítačový program s volně dostupným zdrojovým kódem, který může být volně reprodukován a pozměňován.

[93] *Ransomware as a Service (RaaS) explained*. Crowdstrike [online]. [cit. 2021-5-25]. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/

[94] ZAHARIA, Andra. *Security Alert: New and Cheap Stampado Ransomware for Sale on the Dark Web*. Heimdal security [online]. [cit. 2021-5-25]. Dostupné z: https://heimdalsecurity.com/blog/security-alert-stampado-ransomware-on-sale/

[95] *Darknet* je skrytá část internetu dostupná pouze prostřednictvím specializovaného software, jako je *Tor Browser*.

[96] MELAND, Per Hakon, BAYOUMY, Yara Fareed Fahmy, SINDRE, Guttorm. *The Ransomware-as-a-Service economy within the darknet*. Computers & Security. 2020 (February). ISSN 0167-4048. Dostupné z: https://doi.org/10.1016/j.cose.2020.101762

O odlišném obraze rozšířenosti trendu RaaS vypovídají práce jiných autorů. Strom[97] ve svém článku z března 2021 jmenuje příklady aktuálně nejvýznamějších RaaS skupin. Mezi rozvíjející se nováčky na trhu řadí RaaS skupiny *Exorcist*, *Lolkek* a *Rush*. Skupiny *Darkside*, *Thanos* a *Clop* označuje za rostoucí hráče s několika úspěšně provedenými útoky a funkčními blogy sloužící k „*naming and shaming*“[98] těch obětí, které odmítly výkupné zaplatit. Mezi vrcholové organizace s množstvím veřejné známých útoků, které jsou v hledáčku orgánů činných v trestním řízení, podle Stroma patří skupiny stojící za *Ryuk*[99], *REvil* a *DoppelPaymer*. Společnost Intel471[100], která se zabývá bojem proti kybernetické kriminalitě, vypracovala obsáhlejší seznam 25 RaaS skupin, jejichž činnost sledovala v průběhu roku 2020. Za nejvýznamější skupiny označuje *DoppelPaymer*, *Egregor/Maze*, *Netwalker*, *REvil* a konečně *Ryuk*. *Ryuk*, s nejvyšší pravděpodobností skupina hackerů ruské národnosti, byla podle informací společnosti Intel471 zodpovědná za miliony ransomware incidentů po celém světě.[101] Údajně by mohlo jít o 1/3 všech ransomware útoků, které se odehrály v roce 2020. Podle NÚKIB byl v květnu 2021 v České republice aktuální hrozbou zejména pro soukromé společnosti a organizace RaaS *Avaddon*, který v sobě kombinoval šifrovací ransomware a doxware.[102]

S ohledem na výše uvedené lze říci, že RaaS jako kyberkriminální trend skutečně je významnou globální bezpečnostní hrozbou. Výrazná profesionalizace největších hráčů na poli RaaS, technická propracovanost ransomware programů jako je *Ryuk* a široké možnosti financování tohoto typu kriminální činnosti je obzvláště v době globální pandemie citelným problémem, a to mimo jiné vzhledem ke skutečnosti, že jsou čím dál častějším cílem útoků těchto skupin právě nemocniční zařízení.[103]

---

[97] STROM, David. *The rise of ransomware as a service*. Avast Blog [online]. [cit. 2021-5-25]. Dostupné z: https://blog.avast.com/ransomware-as-a-service-avast

[98] V překladu z angličtiny *jmenování a očerňování*.

[99] Ransomware Ryuk byl mimo jiné zodpovědný za útok na nemocnici v Benešově v roce 2019. Zdroj: *Za útokem na benešovskou nemocnici byl ruský vir Ryuk*. ČT24 [online]. [cit. 2021-5-30]. Dostupné z: https://ct24.ceskatelevize.cz/regiony/stredocesky-kraj/3029729-za-utokem-na-benesovskou-nemocnici-byl-rusky-vir-ryuk

[100] *Ransomware-as-a-service: The pandemic within a pandemic*. Intel471 [online]. [cit. 2021-5-30]. Dostupné z: https://intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/

[101] Tamtéž.

[102] Národní úřad pro kybernetickou a informační bezpečnost ČR. *Upozornění na probíhající kampaň ransomwaru Avaddon* [online]. [cit. 2021-5-30]. Dostupné z: https://www.nukib.cz/cs/infoservis/hrozby/1717-upozorneni-na-probihajici-kampan-ransomwaru-avaddon/

[103] Nejčastěji se jedná právě o ransomware Ryuk. Zdroj: *Hospitals Targeted in Rising Wave of Ryuk Ransomware Attacks*. Check Point [online]. [cit. 2021-5-30]. Dostupné z: https://blog.checkpoint.com/2020/10/29/hospitals-targeted-in-rising-wave-of-ryuk-ransomware-attacks/

2 Kriminologické aspekty šíření ransomware

Z pohledu kriminologie je kybernetická kriminalita obtížnou matérií. Tradiční zločin se odehrává v konkrétním čase na konkrétním místě, což dává kriminologům možnost zločin zkoumat v kontextu určitého území a napomáhat například při tvorbě trestní politiky daného státu. Jak již bylo uvedeno výše, kybernetická kriminalita stejně jako kyberprostor nejsou omezeny hranicemi konkrétního státu, není tak snadné zjistit stav, strukturu ani dynamiku kybernetické kriminality na území České republiky. Navíc se bavíme o kriminalitě s vysokou mírou latence[104], policejní, soudní ani vězeňské statistiky tak většinou věrně nereflektují skutečný obraz tohoto typu kriminality na našem území. Rovněž nalézáme problémy v oblasti kriminologické etiologie. Mnoho kriminologických teorií popisující důvody vzniku kriminálního chování přisuzují velký význam prostředí, ve kterém zločin vzniká. V případě kyberprostoru se však jedná o prostředí v přeneseném slova smyslu, neexistuje zde geografická vzdálenost, kulturní rozdíly se do jisté míry stírají a vzniká nová kultura, globální internetová kultura. Disociační aspekt kyberprostoru v kombinaci s vysokou mírou anonymity dává okusit jeho uživatelům pocit, že mohou být někým jiným, dává jim příležitost vyzkoušet jiné sociální role bez rizika ztráty společenského postavení ve skutečném životě.[105] Dle Jaishankara se tak můžeme bavit o zcela jiné množině pachatelů, než jsou pachatelé offline kriminality.[106]

Odborná veřejnost se shoduje, že podstatným kriminologickým jevem v posledních letech je přesun zločinu do kyberprostoru.[107] Nelze se tomuto vývoji divit, zločin v kyberprostoru je často velmi snadno realizovatelný, vysoce efektivní, zároveň spojený s nízkým rizikem odhalení a dopadení pachatele. Tyto jevy, tedy zvyšující se podíl kriminality prováděné v kyberprostoru a obtížnost odhalování a vyšetřování těchto trestných činů, působí ve vzájemné synergii, kdy se v důsledku vysoké latence kybernetické kriminality a nízké objasněnosti kybernetických trestných činů zvyšuje motivace pachatelů své kriminální jednání realizovat právě v kyberprostoru, zatímco orgány činné v trestním řízení nedokáží tento druh kriminality účinně potírat, jelikož se zvyšujícím

[104] Otázkou příčin latence kriminality se budu podrobněji zabývat v kapitole 2.2.
[105] JAISHANKAR, Karupannan. *Space transition theory of cyber crimes*. In SCHMALLEGER, Frank, PITTARO, Michael. *Crimes of the Internet*. New Jersey: Prentice Hall. 2008. ISBN: 978-0132318860. s. 283−301.
[106] Tamtéž.
[107] Již v roce 2018 o tomto trendu mluvil například tehdejší Nejvyšší státní zástupce, Pavel Zeman. Zdroj: Nejvyšší žalobce Zeman: *Zločinci se přesouvají do kyberprostoru*. Novinky.cz [online]. [cit. 2021-6-1]. Dostupné z: https://www.novinky.cz/domaci/clanek/nejvyssi-zalobce-zeman-zlocinci-se-presouvaji-do-kyberprostoru-18402

se množstvím kybernetické kriminality dochází k jejímu technologickému zdokonalování a ke snižování množství stop vedoucí kriminalisty k odhalení útočníků.

Nízká efektivita tradičních prostředků státní moci v boji proti kriminalitě přináší extrémně vysoký význam prevenci na úrovni jednotlivého uživatele či organizace. Představme si na chvíli situaci, kdy by orgány státu neuměly nebo nemohly účinně potírat například vykrádaní bytů. Se zvyšujícím se počtem vykradených počtů by došlo k ekonomickému a technologickému rozvoji výrobců soukromých kamerových systémů, alarmů a bezpečnostních zámků. Každá domácnost ve větších městech by pravděpodobně vlastnila minimálně alarm a trezor, zároveň by se však změnilo i samotné chování obyvatel, kdy by byli opatrnější například při odemykání a zamykání vchodových dveří. V případě kybernetické kriminality však metody prevence nejsou pro spoustu uživatelů natolik intuitivní, jako je tomu u prevence tradiční kriminality. Ačkoliv téměř každý osobní počítač či chytrý telefon dnes má poměrně pokročilé bezpečnostní řešení, často dochází k infikaci počítače škodlivým kódem či k odcizení dat nebo finančních prostředků za určitého přičinění nic netušícího uživatele. Může za tím stát nevhodně nastavené přístupové heslo, nedostatečná záloha dat i podlehnutí určitému typu sociálního inženýrství. Z toho důvodu je u kybernetické kriminality natolik důležitá osvěta a šíření zásad bezpečného chování na internetu. V případě ransomware, u kterého jsou možnosti odvrácení škod po již proběhlém útoku jen velmi omezené, je význam prevence o to větší.

2.1 Hacker culture a její kriminologický význam

Pro správné pochopení příčin a specifik kybernetické krimality a konkrétně šíření ransomware, stejně jako pro poznání pachatele tohoto typu kriminality, je třeba nejprve představit termín *hacker culture*[108] a popsat jeho význam z hlediska kriminologie. Pojem *hacker* bývá v běžné řeči a v médiích často nesprávně užíván pro člověka, který používá své znalosti z oblasti informačních technologií a programování k páchání trestné činnosti. Dle Koloucha je však slovo hacker označením pro osobu s vynikajícími znalostmi fungování informačních a komunikačních systémů, hackeři jsou zdatnými programátory schopnými pracovat ve velmi krátkém čase. Jednou z dovedností hackera je přitom schopnost získat přístup k počítačovému systému jiným než běžným způsobem, a to za pomoci jím navržených postupů či nástrojů.[109] Co hackera dále odlišuje

[108] Překlad (z angličtiny) *kultura hackerů*.
[109] KOLOUCH, Jan. *CyberCrime*. 2016. op. cit. s. 272.

od běžného odborníka na informační a komunikační technologie je jeho zakotvení v určitém ideovém a komunitárním rámci, který lze označit právě jako hacker culture.

Castells[110] v roce 2001 rozdělil internetovou kulturu do čtyř vrstev, které se do jisté míry vzájemně prolínají nebo ze sebe vycházejí. *Techno-meritokratická kultura*[111], která je pevně svázaná s akademickými kořeny internetu, staví na idee, že nejvyšší hodnotou je poznání a pokrok. Hodnotícím měřítkem úspěchu pro tuto kulturní vrstvu je *peer review*[112], stejně jako je tomu v akademické sféře. Z akademické sféry byl převzat rovněž princip otevřenosti výzkumu a možnost při vlastním bádání vycházet ze závěrů předchozích autorů a tyto závěry modifikovat. Z této vrstvy kultury internetu se postupně vytvořila druhá vrstva, a to právě hacker culture. Mezi zbylé dvě vrstvy Castells zařadil *virtuální komunitaristy*[113] a *podnikatele*[114]. Hacker culture se podle Castellse vyznačuje kombinací určitých myšlenek a hodnot, ze kterých lze zdůraznit především princip svobody a nezávislosti na institucích a autoritách, zdůrazňování významu poznání a neomezeného bádání a open-source mentalitu. Pro pochopení jejího ideového rámce je stěžejní dílo Stevena Levyho, který v roce 1984 sepsal v několika bodech základní normativní rámec hackerské etiky:

„*1. Přístup k počítačům a čemukoliv dalšímu, co tě může naučit něco o tom, jak svět funguje, by měl být neomezený a absolutní. Vždy respektuj pravidlo osobní zkušenosti.*

2. Veškeré informace by měly být bezplatné.

3. Nevěř autoritám, podporuj decentralizaci.

4. Hackeři by měli být souzeni podle svých činů a nikoliv podle scestných kritérií jako jsou věk, rasa či postavení.

5. Na počítači můžeš vytvářet „krásu“.

6. Počítače mohou změnit tvůj život k lepšímu.“[115]

---

[110] CASTELLS, Manuel. *The Internet Galaxy*. New York: Oxford University Press, 2001. ISBN 0-19-924153-8. s. 36 – 61.
[111] V originále *techno-meritocratic culture*.
[112] Do češtiny lze přeložit jako recenzní řízení, resp. recenze nebo posouzení.
[113] V originále *virtual communitarian culture*. Dle Castellse tato vrstva přinesla do světa internetu sociální aspekt, Zprvu se jednalo především o diskusní a chatovací fóra a určitým směrem zaměřené komunity. Dnes bychom za vrcholný projev této kulturní vrstvy internetu mohli označit globální sociální sítě, jako je Facebook, Twitter či Instagram.
[114] V originále *entrepreneurial culture*. Jedná se o internetový svět byznysu. Za ztělesnění této kulturní vrstvy byla dlouho považována společnost Microsoft, dnes můžeme zmínit společnosti Google, Amazon a Facebook.
[115] LEVY, Steven. *Hackers: heroes of the computer revolution*. New York: Penguin Books, 2001. ISBN 0-14-100051-1. Český překlad: KOLOUCH, Jan. *CyberCrime*. 2016. op. cit. s. 270.

Vysoký důraz na význam bádání bez ohledu na případný finanční přínos a ochota sdílet vlastní práci s ostatními členy komunity, stejně jako zjevný prvek meritokracie v rámci hackerské komunity, zřejmě pochází z akademických kořenů, na kterých základy hackerské kultury vyrostly.

Jak již bylo uvedeno, definičním znakem hackera není kriminální či jinak společensky škodlivá činnost. Nezanedbatelná část hackerů je však spojena se společensky nežádoucí činností, která může mít i trestněprávní důsledky. Tuto část hackerské komunity označujeme jako *crackers*[116] či *black hats*[117]. Black hat hackeři prolamují bezpečnostní opatření počítačových systémů za účelem vlastního prospěchu či za účelem následného prodeje zjištěné zranitelnosti, přičemž nehledí na materiální škody, které v důsledku jejich jednání jiným osobám vznikají. Opakem jsou *white hats*[118], což jsou hackeři, kteří prolamují bezpečnostní opatření systémů na základě dohody s jejich provozovateli, tato činnost slouží ke zdokonalování bezpečnostních systémů. Mezi nimi stojí *grey hats*[119], kteří střídají legální činnost s činností nelegální.

Z hlediska geneze kriminality v prostředí internetu je významná rozdílnost hodnot hackerské komunity oproti většinové společnosti. Mezi hackerskou komunitou je vzhledem k její odborné povaze a poměrně velké nepřístupnosti pro běžného jednotlivce časté pohrdání jinými méně technicky vzdělanými uživateli počítačových systémů.[120] Dokazování technické a intelektuální nadřazenosti vůči těmto osobám (ale i vůči institucím či orgánům státu) může spočívat právě i v infikaci zařízení takovéhoto uživatele škodlivým kódem (například právě ransomwarem) či v jiném způsobu prolamování bezpečnostních opatření takového uživatele. Významným prvkem je také nedůvěra či dokonce až nenávist vůči autoritám a s ní související pocit, že hackerská etika je spravedlivější a legitimnější než většinová společenská pravidla a právní normy.[121] Mezi jednotlivými skupinami v hackerské komunitě může v důsledku ideové či technologické rozdílnosti docházet ke vzájemné nevraživosti a kmenové mentalitě.[122] Z kriminologického hlediska tak lze do jisté míry hackerskou komunitu (převážně právě black hats komunitu) označit za subkulturu[123].

---

[116] Z anglického slova *to crack* (louskat, prasknout)
[117] V překladu (z angličtiny) *černé klobouky*.
[118] V překladu (z angličtiny) *bílé klobouky*.
[119] V překladu (z angličtiny) *šedé klobouky*.
[120] O tom hovoří ostatně i Castells. CASTELLS, Manuel. *The Internet Galaxy*. 2001. op. cit. s. 49.
[121] Můžeme zmínit například činnost nejznámějšího hackerského hnutí *Anonymous*, které podniká kybernetické útoky proti jednotlivcům, společnostem, ale i orgánům veřejné moci, jejichž činnost považuje za škodlivou či amorální.
[122] CASTELLS, Manuel. *The Internet Galaxy*. 2001. op. cit. s. 48.
[123] *Subkulturou* rozumíme část společnosti s opačným hodnotovým rámcem, než je hodnotový rámec většinové společnosti. Subkultura bývá spojována s delikventním chováním.

2.2 Jaké jsou příčiny vzniku kriminálního chování spočívajícího v šíření ransomware a kdo je pachatel

Jak bylo uvedeno v předchozí kapitole, pro správnou analýzu důvodů vzniku ransomware je nutné přihlížet ke kriminologickému významu hackerské subkultury. Ještě do nedávné doby totiž šíření malware, a to ani v případě ransomware, nebylo přes svou technologickou vyspělost účinným způsobem, jak vydělávat peníze. Ostatně, jak již bylo výše uvedeno, ani veleúspěšný globální kybernetický útok ransomwarem *WannaCry* podle dostupných informací nepřinesl svým autorům velké bohatství. Na fenomén šíření ransomware, ostatně stejně jako i na jiné typy kybernetické kriminality páchané black hats hackery, lze pohlížet optikou **teorií subkultur**[124], které navazují na klasickou **teorii napětí**[125] Roberta Kinga Mertona. Dle Mertona zločin vzniká v důsledku napětí mezi společností obecně přijímanými cíli a k nim vedoucími prostředky, které jsou buď legitimní, avšak nejsou dostupné všem členům společnosti, nebo jsou z hlediska většinové společnosti zavrhovány.[126] Dle teorie subkultur v důsledku tohoto tlaku vzniká skupina podobně znevýhodněných osob, které se pro naplnění těchto jim těžko dosažitelných cílů stanou součástí subkultury. Subkultura se přitom vyznačuje obrácením hodnotového rámce většinové společnosti.[127] Obtížně dosažitelným cílem může být kromě finančních úspěchů například společenské uznání a pocit sounáležitosti. Nemusí se přitom jednat o materiální či intelektuální znevýhodnění, tímto znevýhodněním může být například sociální vyloučení z důvodu odlišnosti či nesoulad zájmů a hodnot se zájmy a hodnotami většinové společnosti. To může být obecně jednou z příčin vzniku hackerských komunit, a to nejen těch, které jsou zaměřené na nelegální činnost. Společensky škodlivé jednání v podobě tvorby a šíření ransomware v případě členů black hats komunit může jejím členům přinášet benefity v podobě postupu na hierarchickém žebříčku, uznání a pochvaly v rámci meritokratického systému takové komunity, kterých by se jim v rámci systému sociální hiearchie většinové společnosti nedostávalo.

Ačkoliv nelze popírat existenci určité míry konfliktu mezi hackerskou kulturou (obzvláště black hat části hackerské komunity) a většinovou kulturou, je nutné vzít na vědomí skutečnost, že členové hackerských komunit nežijí výlučně v rámci své subkultury, ale každodenně se účastní

---

[124] Významnými představiteli teorie subkultur byli Albert Cohen, Richard Cloward a Lloyd Ohlin.
[125] V originále *strain theory*.
[126] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ, Iveta a kol. *Kriminologie. 5. aktualizované vydání.* 2019. op. cit. s. 65.
[127] MUNKOVÁ, Gabriela. *Sociální deviace. Přehled sociologických teorií*. Plzeň: Aleš Čeněk. 2013. ISBN: 978-80-7380-398-8. s. 57.

sociálních interakcí v běžné společnosti v rámci vlastního offline života. Hackeři jsou tak každodenně konfrontování většinovou nedeviantní společností a jejími normami. David Matza ve své knize *Delinquency and Drift* oponuje klasické teorii subkultury Alberta Cohena, když říká, že členové subkultury nejsou zcela odproštěni od hodnotového rámce běžné společnosti a takříkajíc *driftují* na základě vlastní vůle, zda se v dané chvíli budou chovat deviantně či nikoliv.[128] K odproštění se od morálních problémů, které optikou většinové společnosti při páchání kriminality vznikají, používají delikventi podle Matzy a Sykese metody tzv. *neutralizace*, které představují jakési ospravedlňování či racionalizaci vlastního deviantního chování.[129] Podle tohoto pojmu označujeme tuto teorii jako **teorii neutralizace**[130]. Uvedená teorie se dá v jisté míře uplatnit i na námi řešenou problematiku, hackeři mohou driftovat mezi etickým white hat hackingem a black hat hackingem a mohou se nacházet v šedé zóně mezi nimi jako grey hat hackeři. Jako neutralizační technika může sloužit například pokřivený výklad samotné hackerské etiky[131], kdy si mohou grey hats nebo black hats hackeři racionalizovat vlastní kybernetické útoky tím, že jde o boj proti zkaženému systému, který je podle nich postaven na nesprávných hodnotách, či o projev odporu vůči tradičním autoritám.[132] Dle Williamse může vzhledem k disociační povaze kyberprostoru neutralizace kybernetických zločinů spočívat i v popírání existence oběti, kdy útočník své jednání racionalizuje tak, že sám sobě nalhává, že „*na druhém konci nikdo není*“ či „*že to není skutečné*“.[133] Rovněž mohou útočníci vnímat své oběti jako osoby, které příliš nedbají o vlastní kybernetickou bezpečnost či nemají dostatečnou počítačovou gramotnost a vlastní útok považují za jakousi výchovnou lekci hrozby ignorujícího uživatele.

Z hlediska kapitalizace šíření ransomware a možnosti zbohatnutí na tomto typu kriminality byla významná zejména poslední léta, kdy docházelo k masivní komercializaci tohoto kriminálního sektoru v důsledku rozšiřování trendu RaaS a v důsledku zefektivňování kybernetických útoků cílením na finančně lákavé cíle. Jinými slovy, šíření ransomware se začalo vyplácet[134] a možnost páchání tohoto typu kriminality se otevřela i technicky méně zdatným

---

[128] MATZA, David. *Delinquency and Drift*. London: Routledge. 1990. ISBN: 978-0887388040.
[129] SYKES, Gresham M‘Cready, MATZA, David. *Techniques of Neutralization: A Theory of Delinquency*. American Sociological Review. 1957, 22(6). ISSN 00031224. Dostupné z: doi:10.2307/2089195
[130] V originále *neutralization theory*.
[131] MORRIS, Robert G., *Computer Hacking and the Techniques of Neutralization: An Empirical Assessment*, 2010. [online]. [cit. 2021-6-14]. Dostupné z: doi: 10.4018/978-1-61692-805-6.ch001
[132] Příkladem může být činnost již zmiňované skupiny *Anonymous*.
[133] WILLIAMS, Matthew. *Virtually criminal: Crime, deviance and regulation online*. London: Routledge. 2006. ISBN: 978-0-415-36405-8. s. 43.
[134] Jen skupina REvil si podle informací společnosti IBM za rok 2020 na ransomware vydělala více než 123 milionů dolarů. IBM SECURITY. *IBM X-Force Threat Intelligence Index. 2021*. [online]. [cit. 2021-6-18]. Dostupné z: https://www.ibm.com/security/data-breach/threat-intelligence. s. 5.

uživatelům. V této době již nelze ve všech případech zaměňovat pachatele šíření ransomware s black hat hackery, kteří dnes působí primárně jako vývojáři malware či tvůrci exploitů a různých forem sociálního inženýrství. Pachatelé šíření ransomware se mohou rekrutovat například z hospodářských konkurentů napadaných společností, kteří se úspěšným útokem snaží snížit reputaci svého konkurenta, způsobit mu hospodářskou ztátu či se na něm obohatit. Zákazníky i provozovateli RaaS jsou rovněž zavedené kriminální organizace, pro které je kybernetický zločin jen jednou z položek jejich kriminálního portfolia.[135] Zcela odlišnou skupinou útočníků jsou pak *script kiddies*[136], tedy útočníci s malým technickým talentem, kteří provádějí útoky za pomoci již vyvinutých ransomware programů. Vzhledem ke skutečnosti, že nevyvíjejí vlastní škodlivé kódy, je tento typ útoku často jednoduše odhalitelný antivirovými programy, účinnost takových útoků nebývá vysoká. Rovněž se vzhledem k amatérskému způsobu útoků nelze bavit primárně o finační motivaci těchto pachatelů, spíše jim lze přisuzovat jako hlavní motivátory *thrill-seeking*[137] či zvědavost.

Vzhledem ke zvláštní povaze kybernetického zločinu je nutné zohlednit, že mimo svou identitu v kyberprostoru mohou pachatelé šíření ransomware vést zcela běžný život, který nemusí být spojen s pácháním jakékoliv jiné kriminality. Výše uvedené teorie jsou sice aplikovatelné mimo jiné na kriminální chování v kyberprostoru, nezohledňují však veškerá jeho kriminologicky významná specifika a neodpovídají na otázku, zda a do jaké míry se překrývá množina pachatelů ve fyzickém světě a množina pachatelů v kyberprostoru. Dostáváme se tak ke kriminologické teorii, která je výlučně zaměřená na kybernetickou kriminalitu, a to ke **space transition theory**[138], jejímž tvůrcem je indický kriminolog Karuppannan Jaishankar. Základní postuláty space transition theory jsou následující:

„1. Osoby s potlačeným kriminálním chováním (ve fyzickém světě) mají sklon k páchání zločinu v kyberprostoru, který by z důvodu svého sociálního statutu a postavení ve fyzickém světě nespáchali.

2. Flexibilita identity, disociativní anonymita a nedostatek odstrašujícího faktoru v kyberprostoru poskytují pachatelům příležitost spáchat kybernetický zločin.

---

[135] Příkladem může být probíhající fůze tradičních mafií s hackerskými skupinami. Více na: GLENNY, Misha. *Cybercrime is becoming the mafia's newest racket*. Roland Berger [online]. [cit. 2021-6-18]. Dostupné z: https://www.rolandberger.com/en/Insights/Publications/Cybercrime-is-becoming-the-mafia%E2%80%99s-newest-racket.html

[136] Volně přeloženo z angličtiny jako *skriptovací děti*.

[137] V překladu z angličtiny *hledání vzrušení*.

[138] Volně přeloženo z angličtiny jako *teorie přesunu mezi prostory*.

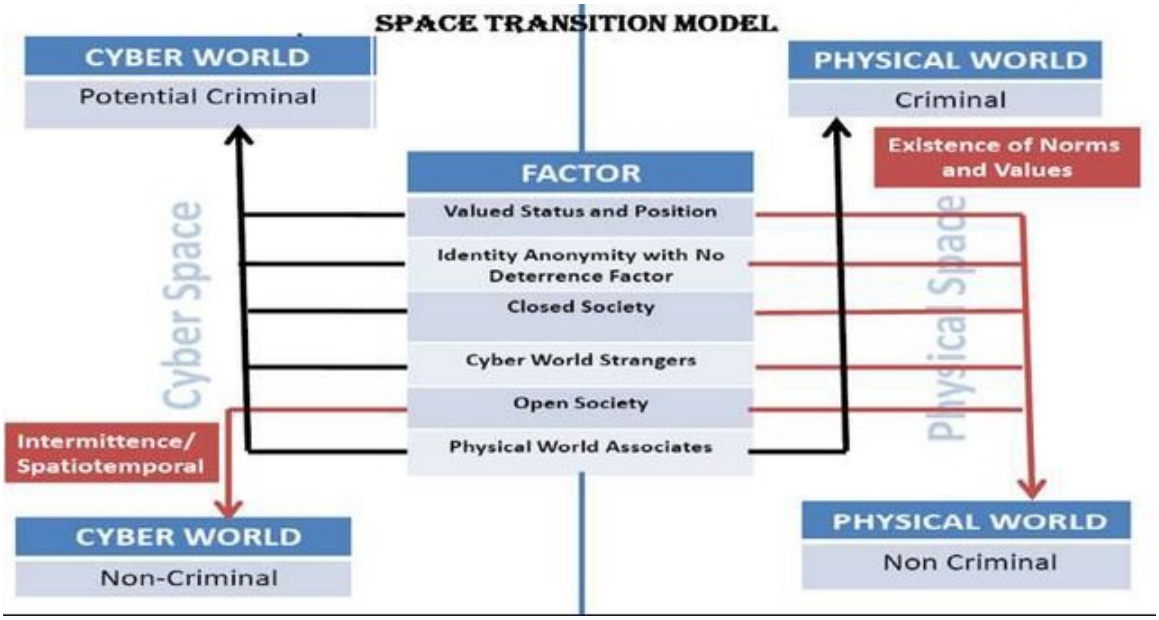
3. Kriminální chování pachatelů v kyberprostoru může být přeneseno do fyzického světa a naopak, kriminální chování ve fyzickém světě může být přeneseno do kyberprostoru.

4. Dočasnost vniknutí pachatelů do kyberprostoru a dynamická časoprostorová povaha kyberprostoru umožňují pachatelům uniknout případnému potrestání.

5. Pachatelé, kteří se vzájemně neznají, se mohou spolčit v kyberprostoru ke společnému spáchání zločinu ve fyzickém světě. Společníci ve fyzickém světě se mohou spolčit ke spáchání zločinu v kyberprostoru.

6. U osob žijících v nesvobodné společnosti je větší pravděpodobnost spáchání zločinu v kyberprostoru než u osob žijící ve svobodné společnosti.

7. Rozpor mezi normami a hodnotami fyzického světa a normami a hodnotami kyberprostoru mohou vést ke kybernetickému zločinu.“[139]



Obrázek 4 – Model space transition theory[140]

První a druhý postulát space transition theory nám říká, že v případě kybernetického zločinu pracujeme i s pachateli, kteří by ve fyzickém světě trestnou činnost nepáchali. Osoby

[139] JAISHANKAR, Karuppannan. *Space transition theory of cyber crimes*. 2008. op. cit. s. 292. Z angličtiny přeloženo autorem.
[140] Zdroj: https://www.researchgate.net/publication/321716315_Space_Transition_Theory_of_Cyber_Crimes

s potlačenými kriminálními sklony, které trestnou činnost ve fyzickém světě nepáchají z obavy o ztrátu vlastní společenské pozice, tuto obavu v prostředí kyberprostoru nemají či je zásadním způsobem redukovaná. Anonymita kyberprostoru se dá připodobnit k masce, která pachatele chrání před odhalením skutečné identity, přičemž zároveň působí disinhibičně.[141] Pachatelé tak ztrácejí zábrany z důvodu nepřítomnosti účinného strážce, přičemž ztráta zábran se může projevovat právě i společensky škodlivým jednáním. Anonymita a flexibilita identity v kyberprostoru, která je často reprezentovaná jen vybranou přezdívkou a vizuálním stvárněním virtuální identity, avatarem, jakož i abstraktní povaha takové identity, pachateli zároveň dává pocit, že není sebou samým. Stejně tak zbavuje pachatele pocitu osobní odpovědnosti za své jednání. Tento jev nazýváme *deindividualizací.* Deindividualizace vede pachatele k méně altruistickému, více sobeckému a agresivnímu jednání. [142]

Výše uvedené postuláty lze uplatnit i na šíření ransomware. Pachatelé šíření ransomware nejsou v přímém nezprostředkovaném styku s obětmi, nejsou tak svědky negativních následků své škodlivé činnosti. Jejich hackerská identita působí disinhibičně a deindividualizačně, prolomení bezpečnostních opatření může působit pouze jako jakási intelektuální výzva, navíc s možností finančního výdělku. Kriminální chování spočívající v šíření ransomware v kyberprostoru může lákat i ty osoby, které by se ve fyzickém světě kriminálního jednání nedopouštěly z obavy o vlastní společenské postavení či z obavy z případných právních následků. Pro ilustraci můžeme uvést skupinu grey hats hackerů, kdy zpravidla nejde o profesionální zločince, tedy takové zločince, jejichž primárním zdrojem příjmů je kriminální činnost, ale jedná se o osoby, které kvůli anonymitě v kyberprostoru a z důvodu ztráty odstrašujícího faktoru čas od času vybočují z legální profesní činnosti k činnosti kriminální. Stejně tak se může jednat o již zmiňované legální komerční společnosti, které se ransomware útokem snaží poškodit svou konkurenci či se na její úkor obohatit.

Postulát o přenosu kriminálního jednání z reálného světa do kyberprostoru v případě šíření ransomware platí primárně pro již zmiňovaný přesun organizovaného zločinu do kyberprostoru. Kyberprostor těmto organizacím přináší nové možnosti výdělku, jako je například právě výkupné z ransomware útoků či poplatek za poskytnutí služby v rámci RaaS. Vzhledem k časté mezinárodní povaze organizovaného zločinu je kyberprostor vhodným prostředím pro svou

[141] JAISHANKAR, Karuppannan. *Space Transition Theory of Cyber Crimes*. 2008. [online]. [cit. 2021-6-15]. Dostupné z: https://www.researchgate.net/publication/321716315_Space_Transition_Theory_of_Cyber_Crimes. s. 7.
[142] JAISHANKAR, Karuppannan. *Space Transition Theory of Cyber Crimes*. 2008. [online]. Op. cit. s. 8.

geografickou nezávislost. Podstatným faktorem jsou i ztížené možnosti vyšetřování kybernetických zločinů.

Zajímavostí je teze o zvýšené pravděpodobnosti vzniku kriminálního chování v kyberprostoru u osob žijících v nesvobodné (či uzavřené) společnosti. Dle Jaishankara lidé v otevřených společnostech mohou legálními prostředky vyjadřovat svou nespokojenost a hněv ve formě protestů a demonstrací, v případě uzavřených společností se skrytá agrese může přesunout do kyberprostoru, kde se může projevovat například ve formě politicky motivovaných útoků či jako kyberterorismus.[143] V tomto směru je významné, že velká část významných hackerských organizací a ransomware skupin pochází z nesvobodných a autoritářských zemí, jako je Ruské federace, Čína, Írán či z KLDR. Je však otázkou, do jaké míry je toto dáno tlakem autoritářské společnosti na svobodu jednotlivců a do jaké míry je tento jev ovlivněn kupříkladu státní podporou těchto aktivit.

S touto problematikou souvisí další aspekt šíření ransomware, který v dosavadním výkladu nebyl příliš zohledněn, a to skutečnost, že se ransomware obzvláště v poslední době stává zbraní v rukou jednotlivých států či teroristických organizací.[144] Ransomware může sloužit také jednotlivcům a nestátním organizacím s politickými či mocenskými cíli. Tento aspekt problému nelze důsledně zkoumat optikou klasických kriminologických teorií, spíše než o kriminologickou otázku se jedná o problematiku mezinárodních vztahů, politologie či dokonce o otázku vojenské vědy. Tomuto tématu se budu blíže věnovat v podkapitole 2.6.3.

2.3 Latence šíření ransomware a její příčiny

Jednou z překážek kriminologického zkoumání šíření ransomware a kybernetické kriminality obecně je vysoká latence tohoto typu kriminality. Uvádí se, že u kybernetické kriminality se míra latence pohybuje mezi 90 až 95 %.[145] Latentní kriminalitou rozumíme takovou množinu spáchaných trestných činů, která tvoří rozdíl mezi skutečnou kriminalitou a kriminalitou registrovanou.[146] Pokud tedy hovoříme o vysoké latenci kybernetické kriminality, znamená to, že

---

[143] JAISHANKAR, Karuppannan. *Space Transition Theory of Cyber Crimes*. 2008. [online]. Op. cit. s. 12.
[144] Kupříkladu o tom hovoří výroční zpráva BIS za rok 2019. Zdroj: Bezpečnostní informační služba. *Výroční zpráva bezpečnostní informační služby pro rok 2019*. 2020. [online]. [cit. 2021-6-15]. Dostupné z: https://www.bis.cz/vyrocni-zpravy/vyrocni-zprava-bezpecnostni-informacni-sluzby-za-rok-2019-c665e2a7.html. s. 10-11.
[145] DIANIŠKA, Gustáv. *Kriminológia*. Plzeň: Aleš Čeněk. 2009. ISBN 978-80-7380-198-4. s. 220.
[146] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ, Ivana a kol. *Kriminologie. 5. aktualizované vydání*. 2019. op. cit. s. 34.

se o vysokém procentu kybernetických trestných činů orgány činné v trestním řízení vůbec nedozví (zde hovoříme o *přirozené latenci* či o tzv. *černých číslech*) či se o nich dozví, ale z nějakého důvodu tyto trestné činy neregistrují (zde hovoříme o *umělé latenci*). O *šedých číslech* hovoříme v případě, že se orgány činé v trestním řízení dozvěděly o trestném činu, avšak se nepodařilo pachatele vypátrat.[147]

Pro kyberkriminalitu obecně platí, že část její latence je způsobena nevědomostí oběti o právě probíhajícím či již proběhlém útoku. Typické je to například při zapojení zařízení do botnetu jako tzv. *zombie počítač*. V případě šíření ransomware toto platí pouze pro některé formy přípravy ransomware útoku, jako je například instalace různých *backdoor*[148] programů, exploitů či rootkitů, které mají umožnit, usnadnit či ukrýt budoucí ransomware útok, či ve chvíli, kdy již došlo k průniku ransomware do počítačového systému, ale dosud nedošlo k jeho aktivaci, respektive k zobrazení ransom note či k omezení funkce systému.

Dalším obecným důvodem latence kybernetické kriminality je obtížnost vyšetřování kybernetické kriminality orgány činnými v trestním řízení a malá pravděpodobnost dopadení pachatele. Pro ilustraci, v roce 2019 činila objasněnost počítačových trestných činů (ve smyslu skutkových podstat dle § 230, § 231 a § 232 TZ) 19,1 %, v roce 2020 klesla objasněnost dokonce až na 12 %.[149]

Dalším důvodem vysoké latence tohoto typu kriminality je skutečnost, že oběť kybernetického trestného činu může nabýt pocitu, že si kybernetický útok přivodila sama svým rizikovým chováním v kyberprostoru a nechce okolnosti útoku řešit s orgány činnými v trestním řízení. Může jít například o sledování pornografického obsahu či stahování nelegálního softwaru a jiného audiovizuálního obsahu, případně vlastní hackerská činnost.

Důvodem nenahlášení kybernetického útoku může být rovněž absence újmy způsobené takovým útokem, což může být případ méně propracovaných či nesprávně zacílených kybernetických útoků.

---

[147] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ, Ivana a kol. *Kriminologie. 5. aktualizované vydání*. 2019. op. cit. s. 35.

[148] *Backdoor* v překladu (z angličtiny) znamená *zadní vrátka*. Jde o metodu obejití bezpečnostních opatření systému za využití softwarového či hardwarového řešení.

[149] *Statistické přehledy kriminality za rok 2019*. Policie ČR [online]. [cit. 2021-6-30]. Dostupné z: https://www.policie.cz/clanek/statisticke-prehledy-kriminality-za-rok-2019.aspx; *Statistické přehledy kriminality za rok 2020*. Policie ČR [online]. [cit. 2021-6-30]. Dostupné z: https://www.policie.cz/clanek/statisticke-prehledy-kriminality-za-rok-2020.aspx

Dalším důvodem, v tomto případě výlučným pro množinu obětí z komerční sféry, je neochota zveřejňovat informace o selhání vlastních bezpečnostních systémů či o úniku nebo ztrátě dat klientů, a to z důvodu možné ztráty kredibility a důvěry mezi vlastními klienty.[150] Společnosti tak mnohem častěji využívají soukromých řešení, namísto tradičního řešení prostřednictvím trestního řízení, které může odhalit jejich slabiny konkurenci a které zpravidla není v této oblasti řešením efektivním.[151] Pachatelé některých typů ransomware útoků, jako je doxware, mohou navíc oběti vydírat zveřejněním citlivých dat, pokud proběhlý kybernetický útok nahlásí příslušným autoritám. I u běžných šifrovacích ransomware útoků obsahem ransom note zpravidla bývá informace, že v případě nahlášení kybernetického útoku policii dojde ke smazání soukromého klíče potřebného k dešifrování dat.

Co se týče důvodů specifických pro ransomware útoky, je třeba zmínit skutečnost, že po úspěšně proběhlém ransomware útoku a po zašifrování dat kvalitní asymetrickou šifrovací metodou orgány činné v trestním řízení zpravidla nemívají efektivní prostředky, jak obětem pomoci s obnovou dat. Mnohem častěji tak dochází k zaplacení výkupného či v lepším případě k obnovení zašifrovaných dat ze zálohy.

2.4 Oběť ransomware útoku

U kybernetické kriminality dochází z viktimologického hlediska k podstatnému momentu, který v kontextu tradiční kriminality není obvyklý. Při páchání běžné kriminality musí zpravidla dojít k protnutí pachatele a cíle útoku v prostoru a čase. Pachatel se tak zpravidla musí setkat na konkrétním místě v konkrétní čas se svou obětí, s jejím majetkem nebo s jinou osobou či předmětem, které mají s obětí souvislost.[152] I v případech, kdy dochází k útoku na dálku, například prostřednictvím poštovní zásilky či telefonního hovoru, ve většině případů musí dojít alespoň k časovému protnutí pachatele a oběti či k nějaké formě překonání geografické vzdálenosti mezi nimi. V případě kybernetických útoků však prostor a čas nemusí hrát žádnou roli. Pachatel a oběť mohou být vzdáleny tisíce kilometrů daleko, k infikaci počítačového systému škodlivým kódem může dojít ve kterýkoliv čas, během zlomku vteřiny od zahájení útoku, ale i ve chvíli, kdy od aktivního jednání útočníka v podobě vytvoření či rozšíření škodlivého kódu uběhlo mnoho hodin, dnů, týdnů i let. Spatiotemporální omezení běžné kriminality obětem zpravidla dává do jisté míry

[150] WALL, David S. *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press. 2007. ISBN: 978-0-7456-2736-6. s. 20.
[151] WALL, David S. *Cybercrime: The Transformation of Crime in the Information Age*. 2007. op. cit. s. 26.
[152] WILLIAMS, Michael. *Virtually criminal: Crime, deviance and regulation online*. 2006. op. cit. s. 19.

možnost se pachateli vyhnout či vlastní viktimizaci předcházet, viktimologům pak dává možnost v kontextu určitého území a času zkoumat viktimnost[153] různých skupin osob, ať už na základě územního, sociálního či třeba profesního klíče. V případě zkoumání obětí kybernetické kriminality je tak nutné zohlednit toto jeho zvláštní specifikum.

Pro efektivní viktimologickou analýzu šíření ransomware je třeba oběti ransomware rozdělit do dvou základních skupin, a to na oběti nahodilé, tedy oběti plošných nezacílených ransomware útoků, a dále na oběti zamýšlené, cílené.[154]

Prvně k obětem nahodilým. Jak již bylo uvedeno výše, pachatelé méně sofistikovaných ransomware útoků si zpravidla své oběti nevybírají, ale snaží se své škodlivé kódy rozšiřovat mezi co největší množství počítačových systémů. Spektrum možných nahodilých obětí je velmi široké, může se jednat o běžné uživatele, nejrůznější právnické osoby, ale například i nemocnice a systémy veřejné správy. Pachatel své oběti nezná, vztah pachatele a oběti je tak v tomto případě zpravidla neexistující. Významným faktorem viktimizace tohoto typu oběti je její rizikové chování. To může zahrnovat navštěvování rizikových webových stránek, kde může docházet k infikaci počítače například prostřednictvím malvertisingu, klikání na podezřelé odkazy, otevírání příloh rizikových e-mailových zpráv, odkládání záplatových aktualizací softwaru a nedostatečné zálohování důležitých souborů a dat. Rizikovým chováním je rovněž používání starých verzí operačních systémů a jiného softwaru, příkladem může být již zmiňovaný dopad šíření ransomwaru WannaCry v roce 2017 na britské nemocnice spadající pod NHS, které z 90 % používaly v té době již zastaralý operační systém Windows XP.[155] U nahodilých obětí obvykle nedochází k velkým majetkovým škodám, pokud se cílem útoku nestanou právě zrovna nemocniční zařízení, zařízení kritické infrastruktury nebo systémy významných společností. Stejně tak požadované výkupné nebývá příliš vysoké, útočníci tohoto typu útoků zpravidla volí strategii *de minimis*, kdy až výsledná agregovaná částka z většího množství útoků dosahuje pro pachatele zajímavějších čísel.[156]

---

[153] Disponovanost jednotlivce či skupiny stát se obětí trestného činu. GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ, Ivana a kol. *Kriminologie. 5. aktualizované vydání.* 2019. op. cit. s. 123.

[154] Podobné rozdělení skupin obětí použil ve své diplomové práci i Johanovský. JOHANOVSKÝ, Tomáš. *Kriminologické a trestněprávní aspekty fenoménu ransomware*. Praha. 2018. Diplomová práce. Univerzita Karlova, Právnická fakulta. Vedoucí práce doc. JUDr. Tomáš Gřivna, Ph. D. s. 30.

[155] KRUPKA, Jaroslav. *Globální kyberútok vyřadil počítače s Windows XP, uvedla britská ministryně*. Deník.cz [online]. [cit. 2021-6-30]. Dostupné z: https://www.denik.cz/ze_sveta/kyberutok-vyradil-pocitace-s-windows-xp-uvedla-britska-ministryne.html

[156] WALL, David S. *Cybercrime: The Transformation of Crime in the Information Age*. 2007. op. cit. s. 3.

Co se týče obětí cílených, zde již můžeme vysledovat určité jednotící charakteristiky. Původci ransomware útoků budou zpravidla cílit na ty subjekty, u kterých se lze důvodně domnívat, že budou schopni a ochotni zaplatit požadované výkupné. Zpravidla se tak bude jednat o podnikatelské subjekty, ale také již zmiňované nemocnice, veřejné subjekty a systémy kritické infrastruktury. Podle studie IBM byla za rok 2020 kybernetickými útoky nejvíce postižena oblast finančnictví a pojišťovnictví, na druhém místě se pak ocitla výroba.[157]

Možnosti prevence takto cíleného kybernetického útoku jsou daleko omezenější než v případě plošných útoků na nahodilé oběti. Útočníci tohoto typu útoků zpravidla používají propracovanější metody průniku přes bezpečnostní systémy oběti. V některých případech, kdy se jedná o útok na velmi lukrativní cíl, či se jedná o útok znepřátelené mocnosti či organizace, se může jednat o APT[158] útočníky, kteří disponují značnými finančními i personálními zdroji a pro prolomení bezpečnostních opatření oběti využívají extrémně propracovaných metod s dlouhodobou přípravou, jako je například spear phishing. Ani přes častá školení zaměstnanců, hloubkové bezpečnostní audity a kvalitní systémy kybernetické bezpečnosti nelze úspěšný ransomware útok nikdy zcela vyloučit.

Jak již bylo uvedeno výše, cílená oběť bude pravděpodobně odrazována od nahlášení kybernetického útoku obavou o vlastní důvěryhodnost v očích vlastních klientů, zároveň se bude často jednat o zašifrování dat s mnohem vyšší hodnotou, než je hodnota požadovaného výkupného. Některým subjektům nedostupnost systémů i v krátkém čase přináší vysoké ekonomické ztráty, například právě v sektoru výroby. Všechny tyto faktory přispívají k rozhodnutí obětí výkupné útočníkům zaplatit.

Relevantní může být rovněž vztah mezi pachatelem a obětí, pachatelem ransomware útoku proti společnosti se může stát například její bývalý či současný zaměstnanec, pro kterého je prolomení bezpečnostních opatření z důvodu důvěrné znalosti těchto systémů snadné.[159] Motivací tohoto typu útočníka může být kromě motivace finanční také touha po pomstě bývalému zaměstnavateli. Rovněž může dojít ke kybernetickému útoku mezi znepřátelenými hackerskými skupinami. Obecně lze říci, že vlastní kyberkriminální aktivita oběti je podstatným faktorem její

---

[157] IBM SECURITY. *IBM X-Force Threat Intelligence Index. 2021.* [online]. [cit. 2021-6-18]. Dostupné z: https://www.ibm.com/security/data-breach/threat-intelligence. s. 5.

[158] *Advanced persisent threat.* V překladu (ang.) *pokročilá trvalá hrozba*. Jde o typ útoku skupinou útočníků, která s vynaložením značných lidských a finančních zdrojů získává neoprávněný přístup k počítačové síti, přičemž zůstává delší dobu nezjištěna. Zdroj: *Pokročilá trvalá hrozba*. Wikipedie [online]. [cit. 2021-6-30]. Dostupné z: https://cs.wikipedia.org/wiki/Pokro%C4%8Dil%C3%A1_trval%C3%A1_hrozba

[159] VLACH, Jiří, KUDRLOVÁ, Kateřina, PALOUŠOVÁ, Viktorie. *Kyberkriminalita v kriminologické perspektivě*. Praha: Institut pro kriminologii a sociální prevenci. 2020. ISBN: 978-80-7338-189-9. s. 83.

vlastní viktimizace. O zvýšené pravděpodobnosti viktimizace členů hackerské subkultury hovoří například Holt a Bossler.[160]

Podstatným fenoménem šíření ransomware z pohledu oběti je opakovaná viktimizace těch obětí ransomware útoků, které se rozhodly v minulosti výkupné zaplatit. Podle studie společnosti Cybereason 80 % obětí, které v minulosti útočníkům zaplatily výkupné, čelily následně dalšímu ransomware útoku.[161] Může se jednat o útok stejné skupiny útočníků, ale také o útok odlišného útočníka, který se o dané společnosti a její ochotě zaplatit požadované výkupné dozví prostřednictvím komunikačních sítí black hat hackerských skupin.

2.5 Prevence ransomware útoku a specifika kybernetické bezpečnosti ve vztahu k ransomware

Jak již bylo uvedeno výše, nejúčinnější metodou boje proti ransomware je prevence. Bez dostatečné opatrnosti a bez dodržování základních zásad kybernetické bezpečnosti existuje poměrně vysoké riziko nákazy zařízení oběti některým typem malware, často pak právě ransomware. V případě úspěšného útok šifrovacím ransomware oběti zpravidla již nezbývá mnoho možností, jak napadená data zachránit.

Základní metodou prevence před útokem ransomware je pravidelná a kvalitní záloha dat. Při existenci kvalitní zálohy útočníci zpravidla i přes úspěšné prolomení bezpečnostních systémů oběti nemají příliš mnoho pák, na základě kterých mohou oběť vydírat. Ačkoliv je moderním trendem provádění zálohy dat prostřednictvím technologie *cloudů*, která vyniká svou jednoduchostí a odolností vůči fyzikálním jevům a přírodním katastrofám jako jsou záplavy či požáry, z hlediska kybernetické bezpečnosti je ideálním řešením uchování důležitých dat na externích zařízeních, které nejsou připojeny k internetu či k nezabezpečené lokální síti. Této metodě ochrany dat se přezdívá *air gap policy*[162]. Na tomto místě je však zároveň nutné dodat, že dnes již existují technologie, které *air gap* mezi zařízením připojeným k internetu a zařízením se zálohou dat dokáží překonat.[163] Dalším způsobem, jak překonat existující zálohu dat, je metoda

---

[160] HOLT, Thomas J., BOSSLER, Adam M. *Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization*. Deviant Behavior. 2008, 30(1), 1-25. ISSN 0163-9625. Dostupné z: doi:10.1080/01639620701876577

[161] *Ransomware: The True Cost To Business*. 2021. Cybereason [online]. [cit. 2021-6-20]. Dostupné z: https://www.cybereason.com/ebook-ransomware-the-true-cost-to-business

[162] V překladu (ang.) *metoda vzdušné bariéry*.

[163] Příkladem malwaru schopného překonat air gap je nástroj *Ramsay* sloužící ke kybernetické špionáži, který objevila a zdokumentovala společnost ESET v roce 2020. SANMILLAN, I. *Ramsay: A cyber-espionage toolkit tailored for*

double extortion[164], kdy útočník oběti vyhrožuje nejen smazáním dat, ale rovněž jejich zveřejněním. Může hrozit nejen zveřejněním citlivých informací či obchodního tajemství konkurenčním společnostem a široké veřejnosti, ale také vystavením osobních dat oběti nebo zaměstnanců oběti na darknetu.

Z hlediska předcházení kybernetickým útokům je zásadní rovněž používání ochranného softwaru. Důležitý je zejména kvalitní antivirový programu s aktuální databází škodlivých kódů a *firewall*[165]. Důležité však je uvědomit si, že ani to nejlepší softwarové řešení stoprocentně nezaručuje, že k infikaci počítače škodlivým kódem nedojde či že bude škodlivý kód spolehlivě rozpoznán. Pokročilé ransomwary mají zpravidla mechanismy, prostřednictvím kterých se dokáží pozornosti antivirových programů vyhýbat, či je dokonce vyřadit z provozu.

Důležitým aspektem prevence nákazy zařízení je tak bezpečné chování uživatele v prostředí internetu. V tomto kontextu lze doporučit používání bezpečných hesel a alespoň dvoufázového ověření identity, vyhýbání se podezřelým webovým stránkám, zachovávání opatrnosti při stahování souborů či softwaru z internetu, nerozklikávání podezřelých odkazů, neotevírání příloh podezřelých e-mailových zpráv a další. Uživatelé by měli dále udržovat veškeré své programové vybavení aktualizované, nezáplatované slabiny softwaru bývají častým vektorem kybernetických útoku.

Co se týče možností prevence u společností a institucí, doporučuje se segmentace sítě, vypnutí maker v nástrojích Microsoft Office a pravidelná školení zaměstnanců o kybernetické bezpečnosti a digitální gramotnosti.[166] Součástí takových školení by mělo být seznámení zaměstnanců s nejrůznějšími phishingovými metodami, ale také například zdůraznění rizik spojených s připojováním externích zařízení do pracovních systémů. Jedním ze způsobů útoků může být totiž pohození USB flash disků se škodlivým kódem na chodbách, v kancelářích a v jiných prostorách potenciální oběti.[167]

---

air-gapped networks. ESET [online]. [cit. 2021-6-20]. Dostupné z: https://www.welivesecurity.com/2020/05/13/ramsay-cyberespionage-toolkit-airgapped-networks/

[164] V překladu (z angličtiny) *dvojí vydírání*.

[165] Hardwarový nebo softwarový prvek sloužící jako brána mezi dvěma sítěmi (například mezi domácí sítí a internetem), který kontroluje komunikaci mezi nimi.

[166] Národní úřad pro kybernetickou a informační bezpečnost ČR. *Vyděračské útoky ransomwarem jsou cílenější: míří na velké firmy, státní a veřejné instituce*. 2020. [online]. [cit. 2021-6-21]. Dostupné z: https://www.nukib.cz/download/publikace/analyzy/Analyza_hrozby_ransomware.pdf

[167] TALAMANTES, Jeremiah. *USB Drop Attacks: The Danger Of "Lost And Found" Thumb Drives*. RedTeam Security [online]. [cit. 2021-6-20]. Dostupné z: https://www.redteamsecure.com/blog/usb-drop-attacks-the-danger-of-lost-and-found-thumb-drives

V případě podezření na právě probíhající ransomware útok by uživatel měl zařízení neprodleně odpojit od internetu a od lokální sítě. Pokud dojde k infikaci zařízení ransomwarem, odborníci zpravidla radí výkupné neplatit.[168] Nejen že neexistuje jistota, že po zaplacení požadované částky dojde ke zpřístupnění zašifrovaných souborů, zaplacením výkupného oběť navíc podporuje kybernetické zločince a financuje jejich další technologický a personální rozvoj. Zároveň se vystavuje riziku dvojí viktimizace, kdy, jak již bylo uvedeno, existuje zvýšená šance ransomware útoku proti těm subjektům, které se v minulosti rozhodly výkupné zaplatit. Na druhou stranu je třeba uvést, že pro mnoho subjektů může být ztráta napadených dat natolik zásadním problémem, že je pro ně i přes nejistotu výsledku výhodnější výkupné zaplatit. Některé ransomware hackerské skupiny navíc budují vlastní „značku“ na důsledném obnovování zašifrovaných souborů po provedení platby.

Možným řešením infikace zařízení některým z již prozkoumaných ransomware je využití činnosti projektu *No More Ransom*. Projekt je společnou iniciativou Nizozemské policie, Evropského centra pro boj proti kybernetické kriminalitě při EUROPOLu, společnosti Kaspersky a společnosti McAfee. Bere si za cíl pomoci obětem ransomware útoku získat zpět zašifrovaná data bez nutnosti platit vyděračům výkupné.[169] Kromě informací o ransomware a preventivních rad, jak útoku předejít, projekt zahrnuje databázi dešifrovacích nástrojů na několik desítek typů ransomware, včetně již zmiňovaných ransomwarů *Avaddon* a *Darkside*. Webová stránka projektu rovněž obsahuje službu *Detektiv Šifra*, která dokáže na základě nahrání některého ze zašifrovaných souborů či po uvedení údajů o útočníkovi (např. adresu jeho Bitcoin účtu) rozpoznat, o jaký typ ransomware se jedná a nabídnout možné řešení.

2.6 Šíření ransomware v souvislosti s aktuálními problémy

Dynamika vývoje ransomware je kromě technologického rozvoje ovlivňována vnějšími faktory, které mohou počet a kvalitu kybernetických útoků akcelerovat. Rovněž lze ve vývoji ransomware pozorovat jisté aktuální trendy, které významným způsobem zvyšují společenskou nebezpečnost tohoto typu kriminality. V této podkapitole představím téma ransomware v aktuálních souvislostech, zaměřím se přitom na téma útoků na nemocnice a jiná zdravotnická

[168] Takové prohlášení vydal i NÚKIB. Zdroj: Národní úřad pro kybernetickou a informační bezpečnost ČR. *Vyděračské útoky ransomwarem jsou cílenější: míří na velké firmy, státní a veřejné instituce*. 2020. [online]. Dostupné z: https://www.nukib.cz/download/publikace/analyzy/Analyza_hrozby_ransomware.pdf. op. cit.
[169] *No More Ransom!* [online]. [cit. 2021-6-22]. Dostupné z: https://www.nomoreransom.org/cs/about-the-project.html

zařízení a s tím spojený vzestup ransomware v době pandemie COVID-19. Dále otevřu problematiku kybernetických útoků řízených státy, otázky kyberterorismu a hacktivismu. Závěrem představím trend, který je potenciálním problémem pro každého koncového uživatele jakéhokoliv *smart* zařízení a který může být do budoucna citelným problémem i při běžném chodu domácnosti, a tím jsou útoky proti IoT[170].

2.6.1 Ransomware útoky na nemocniční zařízení, na systémy veřejné správy a na kritickou infrastrukturu

Jedním z prvních ransomware útoků cílených proti zdravotnickému zařízení byl útok na Presbyteriánské zdravotní středisko v Hollywoodu v únoru roku 2016.[171] Nedlouho po zaplacení požadovaného výkupného napadenou nemocnicí se případy ransomware útoků ve Spojených státech amerických začaly množit. Započal tak extrémně nebezpečný trend, který se nejsilněji projevil v roce 2020 a 2021 v kontextu globální pandemie COVID-19.

Českou stopu trend ransomware útoků na nemocniční zařízení zanechal při útoku na benešovskou nemocnici ransomwarem *Ryuk* 11. prosince 2019. Ač v důsledku tohoto útoku nedošlo k újmě na životě a zdraví pacientů benešovské nemocnice, celkové škody se vyšplhaly na bezmála 60 milionů Kč.[172] Druhým významným incidentem byl útok z března 2020 proti Krajské nemocnici Brno, která v té době prováděla testování vzorků na přítomnost viru SARS-CoV-2.[173]

Rok 2020 se rovněž zapsal do historie kybernetických hrozeb jako rok, kdy došlo k prvnímu úmrtí v souvislosti s kybernetickým útokem. Jednalo se o ransomware útok na nemocnici v německém Düsseldorfu, v důsledku kterého nebyla nemocnice schopna přijímat pacienty. Pacientka tak musela být převezena do několik desítek kilometrů vzdálené nemocnice, kde krátce po přijezdu zemřela.[174]

---

[170] *Internet of Things*. V překladu (ang.) *Internet věcí*. Zapojení všemožných zařízení a spotřebičů (jako jsou chytré ledničky, televizory a automobily) do internetové sítě.
[171] Více informací v dobovém článku: *The hospital held hostage by hackers*. CNBC [online]. [cit. 2021-6-22]. Dostupné z: https://www.cnbc.com/2016/02/16/the-hospital-held-hostage-by-hackers.html
[172] *Středočeští kriminalisté ukončili vyšetřování Ransomware útoku na benešovskou nemocnici.* Policie ČR [online]. [cit. 2021-6-22]. Dostupné z: https://www.policie.cz/clanek/stredocesti-kriminaliste-ukoncili-vysetrovani-ransomware-utoku-na-benesovskou-nemocnici.aspx
[173] HORÁK, Jan. Na nemocnici v Brně zaútočil vyděračský virus, špitál povolal krizového IT manažera. Aktuálně [online]. [cit. 2021-6-23]. Dostupné z: https://zpravy.aktualne.cz/domaci/na-nemocnici-v-brne-zautocil-vyderacsky-virus-spital-povolal/r~ff91a02c6aa011eab1110cc47ab5f122/
[174] *Úmrtí kvůli hackerskému útoku? Byla to jen otázka času, míní bezpečnostní expert.* Novinky.cz [online]. [cit. 2021-6-22]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/umrti-kvuli-hackerskemu-utoku-byla-to-jen-otazka-casu-mini-bezpecnostni-expert-40337662

Nabízí se otázka, proč ransomware útočníci cílí zrovna na nemocniční zařízení. Prvním relevantním faktorem je skutečnost, že zašifrování dat nebo omezení přístupu k nim a přerušení provozu specializovaného zdravotnického vybavení je pro chod nemocnice a pro dostupnost zdravotní péče natolik zásadním problémem, že se nemocnice často rozhodnou výkupné zaplatit. Druhým faktorem je skutečnost, že vybavení a systémy používané v nemocničních zařízeních často běží jako *legacy systémy*[175] na starých verzích operačních systémů, jako jsou Windows 7, Windows Vista a Windows XP, které již nejsou podporovány a aktualizovány výrobcem.

Množí se rovněž útoky proti orgánům státu a územních samospráv a proti kritické infrastruktuře. Podle společnosti Kasperky došlo mezi lety 2018 a 2019 k 60% nárůstu počtu ransomware útoků na systémy územních samospráv, v roce 2019 se počet napadených samospráv vyšplhal na číslo 174, pod které spadá více než 3 000 dalších organizací.[176] V květnu 2021 došlo k rozsáhlému ransomware útoku proti americkému ropnému systému *Colonial Pipeline*, za kterou stála ruská hackerská skupina *DarkSide.*[177] Útok způsobil několikadenní výpadek dodávek benzínu, nafty a dalších ropných produktů na jihovýchodě Spojených států. Server Politico útok označil za pravděpodobně nejzávažnější útok na energetickou infrastrukturu v historii USA.[178]

Co se týče vývoje v České republice, NÚKIB vydal v dubnu 2021, krátce po zveřejnění informace Vládou České republiky o zapojení důstojníků ruské zpravodajské služby GRU při výbuchu muničního skladu ve Vrběticích v roce 2014[179], varování před zvýšeným rizikem kybernetických útoků směřovaných proti České repulice, zejména proti vládním systémům,

---

[175] *Legacy systém* je zastaralý, výrobcem již neaktualizovaný software, který je uživateli i nadále používán. Důvodem může být obtížnost převoditelnosti specializovaných systémů (např. ve zdravotnictví nebo v armádě) na novější verze softwaru.

[176] *Kaspersky research finds 174 municipal institutions targeted with ransomware in 2019*. Kaspersky [online]. [cit. 2021-6-23]. Dostupné z: https://usa.kaspersky.com/about/press-releases/2019_kaspersky-research-finds-174-municipal-institutions-targeted-with-ransomware-in-2019

[177] *Russian criminal group suspected in Colonial pipeline ransomware attack.* NBC News [online]. [cit. 2021-6-23]. Dostupné z: https://www.nbcnews.com/politics/national-security/russian-criminal-group-may-be-responsible-colonial-pipeline-ransomware-attack-n1266793

[178] *'Jugular' of the U.S. fuel pipeline system shuts down after cyberattack*. Politico [online]. [cit. 2021-6-23]. Dostupné z: https://www.politico.com/news/2021/05/08/colonial-pipeline-cyber-attack-485984

[179] *Vyjádření k okolnostem vyhoštění 18 zaměstnanců ruské ambasády*. Vláda ČR [online]. [cit. 2021-6-23]. Dostupné z: https://www.vlada.cz/cz/media-centrum/aktualne/vyjadreni-k-okolnostem-vyhosteni-18-zamestnancu-ruske-ambasady-187806/

významným podnikům a kritické infrastruktuře.[180] Následovaly ransomware útoky proti Magistrátu města Olomouc[181] a proti Národní knihovně ČR.[182]

Stejně jako v případě nemocnic, i v případě systémů státu a územních samospráv, jakož i dalších veřejných systémů, je pravděpodobnou motivací útočníků kombinace poměrně značné zranitelnosti těchto systémů a velké pravděpodobnosti zaplacení požadovaného výkupného, a to z důvodu závažného finančního a společenského dopadu v případě déle trvající nedostupnosti veřejných služeb. Možným vysvětlením útoků proti nemocničním zařízením, proti systémům státu a samospráv, i proti kritické infrastruktuře může být však také snaha o šíření strachu mezi lidmi či motivace přispět ke společenskému rozkolu a k politické nestabilitě.[183] Nelze však opomenout ani skutečnost, že některé nemocnice a další společensky významné subjekty mohou být zasaženy v rámci necíleného plošného ransomware útoku, jak tomu bylo zřejmě i v roce 2017 při útoku *WannaCry*.

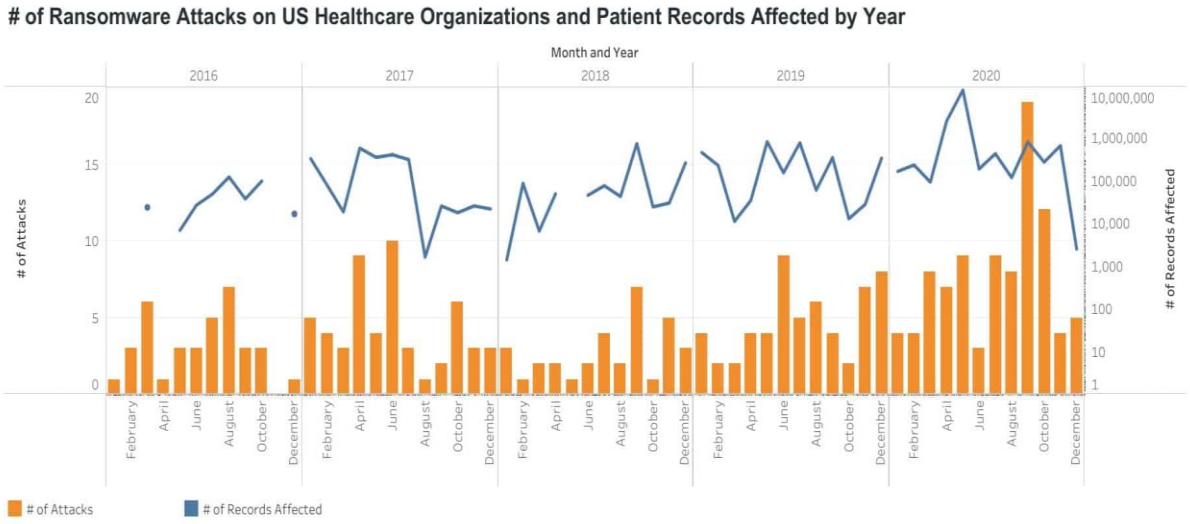
[180] Národní úřad pro kybernetickou a informační bezpečnost. *Upozornění na zvýšené riziko kybernetických útoků proti ČR*. [online]. [cit. 2021-6-23]. Dostupné z: https://www.nukib.cz/cs/infoservis/aktuality/1703-hrozi-zvysene-riziko-kybernetickych-utoku-vuci-ceske-republice/

[181] *Olomoucký magistrát čelí několik týdnů hackerským útokům. Odmítá zaplatit výkupné*. iRozhlas [online]. [cit. 2021-9-2]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/olomouc-magistrat-hackersky-utok-hackeri-ransomware-avaddon_2105221133_ako

[182] *Národní knihovna se stala terčem útoku hackerů. Vedení odstavilo systémy a podalo trestní oznámení*. iRozhlas [online]. [cit. 2021-9-2]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/narodni-knihovna-hackersky-utok_2105181615_pj

[183] O tom více v podbodě 2.6.3.

2.6.2 Ransomware v kontextu pandemie COVID-19



Obrázek 5 – Počet ransomware útoků na nemocniční zařízení (oranžová) a počet napadených lékařských záznamů pacientů (modrá) ve Spojených státech mezi lety 2016 a 2020[184]

Jak lze vidět z uvedeného grafu, počet ransomware útoků na nemocnice ve Spojených státech v roce 2020 vzrostl oproti předchozím letům několikanásobně. Počet útoků proti nemocničním zařízením významně vzrostl i na globální úrovni. Experti tento trend dávají jednoznačně do souvislosti s pandemií COVID-19.[185]

Pandemie COVID-19 posunula závažnost kybernetických hrozeb na novou úroveň, a to zejména co se týče ransomware útoků na zdravotnická zařízení. Bohužel, se zvyšující se závažností a nebezpečností útoků se zvyšuje rovněž ochota zaplatit požadované výkupné a zvedá se i samotná částka, kterou útočníci požadují. Podle EUROPOLu této situace kybernetičtí zločinci využívají tak, že podnikají ransomware útoky ve větší míře a rychleji, rekrutují nové spolupracovníky pro zvýšení dopadu útoků a ve větší míře nabízejí RaaS služby na darknetu.[186] Výsledkem je výrazná finanční a personální expanze tohoto typu zločinného byznysu, která se navenek projevuje právě globálním nárustem počtu ransomware útoků.

[184] Zdroj: https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/
[185] *Global ransomware and cyberattacks on healthcare spike during pandemic*. Bitdefender [online]. [cit. 2021-6-23]. Dostupné z: https://labs.bitdefender.com/2020/05/global-ransomware-and-cyberattacks-on-healthcare-spike-during-pandemic/
[186] *COVID-19 Ransomware*. EUROPOL [online]. [cit. 2021-6-23]. Dostupné z: https://www.europol.europa.eu/covid-19/covid-19-ransomware

Jednou z příčin nárustu kybernetických útoků je zřejmě i masivní přesun pracovníků z kanceláří na *home office*[187], se kterým je vždy nutně spojena zvýšená bezpečnostní hrozba pro zaměstnavatele.[188]

Kybernetičtí útočníci od března 2020, kdy byl Světovou zdravotnickou organizací vyhlášen pandemický stav, rovněž začali masivně používat téma pandemie COVID-19 při svých phishingových kampaních jako způsob distribuce malwaru. Často se jednalo o e-mailové zprávy s infikovanými přílohami tvářící se jako informace o doporučených opatřeních proti koronaviru a o nových lécích adresované nejčastěji orgánům veřejné moci, subjektům podnikajících v pohostinství a službách, výzkumníkům a zdravotníkům, tedy subjektům, které spojoval zájem o co možná nejčerstvější informace o možnostech obrany proti šíření koronaviru. Útočníci se přitom vydávali za významné globální autority jako Světová zdravotnická organizace, NATO nebo UNICEF, případně za národní zdravotnické organizace.[189]

2.6.3 Kyberterorismus, politicky motivované kybernetické útoky a kybernetická válka

Ransomware se kromě nástroje sloužícímu k finančnímu obohacení stává rovněž nástrojem k prosazování politických a mocenských zájmů. Politicky motivované kybernetické útoky a jiné typy hackerské činnosti mohou být projevem občanské nespokojenosti a formou politického protestu, pak hovoříme o tzv. **hacktivismu**. Výhodou kyberprostoru pro politické aktivisty je možnost účasti velkého počtu osob díky geografické nezávislosti kyberprostoru a ochrana před pořádkovými složkami státu, které by fyzickému protestu mohly zabránit blokádami prostoru demonstrace či rozháněním protestujících účastníků.[190] Spojitost mezi hacktivismem a ransomware útoky však nelze jednoznačně nalézt, ačkoliv by tomu mohlo napovídat cílení ransomware útoků na počítačové systémy státu. I tyto útoky zpravidla mají jako primární motivaci výběr výkupného, nesouhlas s politikou daného úřadu či státu však může být motivací vedlejší. Mnohem obvyklejší zbraní aktivistů je přetížení serverů subjektu, proti kterému protest míří,

[187] V překladu *práce z domova*.
[188] *COVID-19 Ransomware*. EUROPOL [online]. [cit. 2021-6-23]. Dostupné z: https://www.europol.europa.eu/covid-19/covid-19-ransomware
[189] ARSENE, Liviu. *5 Times More Coronavirus-themed Malware Reports during March*. Bitdefender [online]. [cit. 2021-6-23]. Dostupné z: https://labs.bitdefender.com/2020/03/5-times-more-coronavirus-themed-malware-reports-during-march/
[190] YAR, Majid. *Cybercrime and society*. London: SAGE Publications, 2006. ISBN 978-1-4129-0753-8. s. 48.

velkým počtem žádostí, které jsou činěny koordinovaně v jeden okamžik.[191] Nejznámější hacktivistickou skupinou je hackerská skupina *Anonymous*.

Politicky motivované útoky mohou být rovněž projevem **kyberterorismu**. Samotný pojem kyberterorismus je velice obtížně definovatelný a žádná definice nebude z principu zcela exaktní, přesto však uvádím definici Dorothy Denningové, podle které je kyberterorismus *„politicky motivovaná hackerská operace, která má za cíl způsobit vážnou újmu, jako je ztráta lidského života či závažná ekonomická ztráta“*[192].

Yar společně s dalšími autory však považuje obraz kyberterorismu jako významné společenské hrozby do jisté míry za mýtizovaný a označuje jej za sociální konstrukt sloužící státním autoritám k politickému ospravedlnění regulace internetu a ke sledování elektronické komunikace. Yar rovněž uvádí, že kybernetický útok na kritickou infrastrukturu je obtížně představitelný, jelikož jsou její systémy zvětšiny izolované od sítě internet. Rovněž argumentuje, že virtualita a imaterialita kybernetických útoků z nich dělá nevhodný prostředek pro šíření teroru.[193]

Aktuální vývoj ransomware útoků a kybernetických hrozeb obecně však vypovídá o opaku. Ransomware útok na americkou potrubní síť *Colonial Pipeline* v květnu 2021, ač jej z důvodu finanční motivace útočníků nelze označit za akt kyberterorismu podle výše uvedené definice, ukazuje možné důsledky kybernetického útoku na běžný chod společnosti na poměrně rozsáhlém území a existenci zranitelnosti kritické infrastruktury vůči vnějšímu útoku z internetu. Časté útoky na nemocniční zařízení zase ukazují možné ohrožení života a zdraví obyvatel z důvodu nedostupnosti zdravotní péče z důvodu kybernetického útoku. Útoky v kyberprostoru tak dle mého názoru dnes již mají potenciál vzbudit strach mezi obyvatelstvem určitého území a jejich původci je mohou činit s politickou motivací.

Podstatným aspektem problému je skutečnost, že kybernetické útoky s motivací dosáhnout politických cílů v dnešním světě často činí přímo orgány některých států či skupiny státy podporované. Tento jev označujeme jako **cyberwarfare**[194]. V současnosti nejznámější hackerskou

---

[191] YAR, Majid. *Cybercrime and society*. 2006 op. cit. s. 48.
[192] DENNING, Dorothy. *Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy*. In: ARQUILLA, John, RONFELDT, David. *Networks and Netwars*. Santa Monica: RAND Corporation, 2001. ISBN 0-8330-3030-2. s. 241.
[193] YAR, Majid. *Cybercrime and society*. 2006 op. cit. s. 56, 61.
[194] V překladu (z angličtiny) *kybernetická válka*, což ovšem není zcela přesné. Zahraniční zdroje zpravidla odlišují pojmy *cyberwar* a *cyberwarfare*, kdy termín *cyberwar* označuje vzájemný konflikt mezi dvěma nebo více státy, který má velký rozsah a intenzitu, přičemž dochází k řadě jednotlivých kybernetických útoků podnikaných všemi

skupinou, která je dle dostupných informací napojená na stát, či je přímo součástí struktury státu, je skupina *Lazarus* z KLDR, americkou vládou přezdívaná jako *Hidden Cobra*.[195] Kromě již výše popsaného globálního ransomware útoku *WannaCry* v roce 2017 má dle dostupných informací *Lazarus* na svědomí ransomware a DDoS útoky proti Jižní Koreji[196], masivní útok proti společnosti Sony Pictures Entertainment a mnoho dalších hackerských akcí po celém světě.[197] Během pandemie COVID-19 skupina *Lazarus* napadala zařízení farmaceutických společností, došlo například k úspěšnému útoku proti britské společnosti *AstraZeneca*, která je jedním z předních evropských výrobců vakcíny proti onemocnění COVID-19.[198] Další hackerské skupiny mají dle dostupných informací napojení na ruské zpravodajské služby (například skupiny *Cozy Bear*[199] a *Fancy Bear*[200]), na íránskou vládu (skupina *Fox Kitten*)[201], na vládu Čínské lidové republiky (mnoho skupin, například *Unit 61398*, která je součástí Čínské lidové armády)[202]. Skupina *Equation*, kterou společnost Kaspersky v roce 2015 označila za pravděpodobně nejvyspělejší hackerskou skupinu světa[203], je podle některých zdrojů součástí americké zpravodajské služby NSA a měla na svědomí vznik exploitu *EternalBlue*, na jehož základě byl později vytvořen ransomware *WannaCry*.[204]

APT skupiny, které, vzhledem k jejich státnímu financování, disponují obrovskými finančními a personálními kapacitami, jsou pro současný svět významnou bezpečnostní hrozbou. Ačkoliv může dojít k dopadení jednotlivých osob, které se na činnosti APT skupin podílí, a k jejich

---

zapojenými stranami konfliktu. *Cyberwarfare* může označovat i ojedinělé kybernetické útoky jediného státního aktéra.

[195] *Lazarus Group*. MITRE ATT&CK [online]. [cit. 2021-6-30]. Dostupné z: https://attack.mitre.org/groups/G0032/

[196] *Andariel evolves to target South Korea with ransomware*. SECURELIST [online]. [cit. 2021-6-30]. Dostupné z: https://securelist.com/andariel-evolves-to-target-south-korea-with-ransomware/102811/

[197] *A Look into the Lazarus Group's Operations*. TrendMicro [online]. [cit. 2021-6-30]. Dostupné z: https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/a-look-into-the-lazarus-groups-operations

[198] STUBBS, Jack. *Exclusive: Suspected North Korean hackers targeted COVID vaccine maker AstraZeneca - sources*. Reuters [online]. [cit. 2021-6-30]. Dostupné z: https://www.reuters.com/article/us-healthcare-coronavirus-astrazeneca-no-idUSKBN2871A2

[199] *Who is FANCY BEAR (APT28)?* Crowdstrike [online]. [cit. 2021-6-30]. Dostupné z: https://www.crowdstrike.com/blog/who-is-fancy-bear/

[200] *Adversary: Cozy Bear*. Crowdstrike [online]. [cit. 2021-6-30]. Dostupné z: https://adversary.crowdstrike.com/en-US/adversary/cozy-bear/

[201] *Fox Kitten – Widespread Iranian Espionage-Offensive Campaign*. ClearSky [online]. [cit. 2021-6-30]. Dostupné z: https://www.clearskysec.com/fox-kitten/

[202] *APT1*. MITRE ATT&CK [online]. [cit. 2021-6-30]. Dostupné z: https://attack.mitre.org/groups/G0006/

[203] *Equation: The Death Star of Malware Galaxy*. SecureList [online]. [cit. 2021-6-30]. Dostupné z: https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/

[204] GOODIN, Dan. *Group claims to hack NSA-tied hackers, posts exploits as proof*. ArsTechnica [online]. [cit. 2021-6-30]. Dostupné z: https://arstechnica.com/information-technology/2016/08/group-claims-to-hack-nsa-tied-hackers-posts-exploits-as-proof/

potrestání prostředky trestního práva jednotlivých zemí[205], je těžko představitelné, že by tímto způsobem mohlo dojít k přerušení činnosti těchto skupin. S přibývajícím napětím v mezinárodních vztazích tak bude logicky přibývat i počet hackerských operací podnikaných znepřátelenými státními aktéry.

2.6.4 Útoky na prvky IoT

Dalším výrazným trendem v ransomware útocích jsou útoky na prvky IoT, jako jsou chytré telefony, spotřebiče, televizory a jiné prvky domácnosti. Čím dál častější využívání prvků IoT v běžném životě ještě více stírá už tak tenkou hranici mezi kyberprostorem a fyzickým světem, kybernetické hrozby jako ransomware v důsledku tohoto trendu přestávají být pouze možným ohrožením dat uživatele, ale stávají se hrozbou také pro jeho offline život.

Ransomware cílící na IoT zpravidla nejsou určena k zašifrování dat uživatele, vzhledem ke skutečnosti, že většina chytrých zařízení neobsahuje pro uživatele významná data (s výjimkou chytrých telefonů), zpravidla se jedná o nějakou formu locker-ransomwarů, které omezí přístup uživatele k zařízení.[206] Zmínit lze kupříkladu ransomware *FLocker*, který zablokuje veškeré ovládací prvky chytrého televizoru a místo audiovizuálního obsahu zobrazí uživateli ransom note, ve kterém se útočník vydává za policejní orgán.[207] *FLocker* je tak IoT podobou klasického policejního viru.

Moderní vývoj kybernetických hrozeb však ukazuje i znepokojivější formy ransomware útoků proti prvkům IoT, které se mohou v nedaleké budoucnosti objevit. Příkladem je ransomware vyvinutý white hat hackery Andrewem Tierneyem a Kenem Munroem, který cílí na chytré termostaty s připojením k internetu. Ransomware po infikaci zařízení změní nastavení termostatu tak, aby došlo k extrémnímu zvýšení teploty v místnosti. Pokud uživatel chce teplotu snížit, musí

---

[205] Například byli americkými úřady obviněni hackeři skupiny Lazarus. Zdroj: MUNCASTER, Phil. *Two More Lazarus Group Members Indicted for North Korean Attacks*. Infosecurity [online]. [cit. 2021-6-30]. Dostupné z: https://www.infosecurity-magazine.com/news/lazarus-group-indicted-north/?__cf_chl_jschl_tk__=pmd_69d42cda2938341282cef6e5cbce05bb5e9cb36e-1626893792-0-gqNtZGzNAfijcnBszQqO

[206] DICKSON, Ben. *The IoT ransomware threat is more serious than you think*. IoT Security Foundation [online]. [cit. 2021-6-25]. Dostupné z: https://www.iotsecurityfoundation.org/the-iot-ransomware-threat-is-more-serious-than-you-think/

[207] ZAHRA, Syed Rameem, CHISHTI Mohammad Ahsan. RansomWare and Internet of Things: A New Security Nightmare. In: 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence). IEEE, 2019, 2019, s. 551-555. ISBN 978-1-5386-5933-5. Dostupné z: doi:10.1109/CONFLUENCE.2019.8776926. s. 553.

zaplatit požadované výkupné.[208] Ačkoliv se jedná pouze o demonstraci možností hackingu IoT zařízení, podobné případy víří fantazii, čím vším lze vlastníky chytrých zařízení vydírat.

Ještě závažnější formy IoT útoků, které se mohou v budoucnu objevovat, jsou útoky na počítačové vybavení chytrých automobilů. Možný kybernetický útok proti ovládacím prvkům automobilu úspěšně demonstrovali Chris Valasek a Charlie Miller již v roce 2015. Tito white hat hackeři využili slabiny v počítačovém systému *Uconnect* automobilu *Jeep Cherokee*, díky které dokázali vzdáleně ovládat řízení automobilu, jeho brzdící systém a další systémy vozidla, a to vše přes internet bez jakéhokoliv přidaného zařízení či úpravy na samotném vozidle.[209] Proti tomuto typu kybernetických útoků varují odborníci již řadu let, například společnost Kaspersky vydala v roce 2018 varování ohledně nedostatečného zabezpečení smart automobilů proti kybernetickým útokům.[210] Podle téže společnosti již dokonce lze nalézt na darknetu reklamy nabízející přístup k hacknutým automobilům[211], je samozřejmě otázkou, do jaké míry jsou tyto reklamy pravdivé. Europol již v roce 2014 varoval před možností smrtelných následků v souvislosti s kybernetickým napadením IoT prvků a před rizikem ransomware programů zaměřených na automobily.[212]

IoT prvky nejsou pouze součásti chytrých domácností a chytré telefony, za prvky IoT jsou považovány například i lékařské přístroje s vlastním síťovým připojením, jako jsou rentgeny, nejrůznější monitorovací zařízení či dýchací přístroje. Množící se ransomware útoky proti nemocničním zařízením se tak do jisté míry překrývají s útoky proti prvkům IoT. Jak již bylo uvedeno výše, tento typ útoku je extrémně nebezpečný, v jeho důsledku může dojít k vážnému ohrožení života a zdraví pacientů či dokonce k úmrtí. Právě vysoká nebezpečnost tohoto typu útoku však vede k častému zaplacení požadovaného výkupného a tedy i k silnější motivaci pachatelů na tyto zařízení cílit.

---

[208] Tamtéž. s. 552.
[209] GREENBERG, Andy. *Hackers Remotely Kill a Jeep on the Highway – With Me in It*. Wired [online]. [cit. 2021-6-25]. Dostupné z: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
[210] GRUSTNIY, Leonid. *Smart cars: Comfort costs.* Kaspersky [online]. [cit. 2021-6-25]. Dostupné z: https://www.kaspersky.com/blog/dont-hack-your-car/22090/
[211] Tamtéž.
[212] TUNG, Liam. *Europol warns of IoT murder and ransomware for smart cars*. ZDnet [online]. [cit. 2021-6-25]. Dostupné z: https://www.zdnet.com/article/europol-warns-of-iot-murder-and-ransomware-for-smart-cars/

2.7 Prognóza budoucího vývoje

Dle Smejkala lze obecně pro oblast kybernetické kriminality v následujících letech očekávat zvýšení počtu útoků na zařízení v rámci rostoucího trendu BYOD[213] a na IoT prvky.[214] Rovněž předvídá větší množství cílených útoků činěných soukromými skupinami pachatelů, které budou mít za cíl majetkové obohacení nebo průmyslovou špionáž. Rovněž lze podle něj očekávat útoky vedené státy, teroristickými organizacemi a útoky ideologicky motivované. Všechny tyto obecné závěry lze vztáhnout na útoky ransomware.

Dále lze předpokládat pokračování trendu útoků na zdravotnická zařízení, vzhledem k jejich dosavadní ekonomické výdělečnosti. Zřejmě lze předpokládat s tím spojený růst cen požadovaného výkupného.

Vzhledem k úspěšnosti aktuálního trendu profesionalizace a čím dál větší zacílenosti útoků ransomware lze očekávat, že i tento trend bude v následujících letech pokračovat. Se zdokonalováním technických prostředků black hat hackerů bude i nadále docházet ruku v ruce ke zdokonalování metod sociálního inženýrství, zejména v podobě spear phishingu.

I podle NCOZ lze v následujícím období předpokládat další nárust ransomware útoků, a to s jednoznačným cílem majetkového prospěchu. Předvídá rovněž zvýšený zájem o průnik zájmových zahraničních skupin do systémů kritické infrastruktury a významných informačních systémů.[215]

Na stranu druhou, se zvyšujícím se procentem společností a institucí, které se již setkaly s nějakou formou hackerského útoku, se bude zvyšovat i povědomí zaměstnanců o kybernetické bezpečnosti a o nejrůznějších phishingových metodách útočníků. Stejně tak se budou i nadále zlepšovat technické prostředky ochrany před kybernetickými hrozbami. I přesto ale nelze očekávat pokles počtu úspěšných ransomware útoků. Technologický vývoj prostředků kybernetických útočníků je vůči vývoji bezpečnostních systémů neustále o krok napřed a jejich vzájemnou

---

[213] *Bring your own device*. V překladu (z angličtiny) *přines si vlastní zařízení*. Moderní trend, kdy zaměstnanci se souhlasem zaměstnavatele přinášejí do kanceláře vlastní zařízení, připojují je k firemní síti a užívají je při práci.

[214] SMEJKAL, Vladimír. *Kybernetická kriminalita. 2. rozšířené a aktualizované vydání*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7. s. 844 - 845

[215] Národní centrála proti organizovanému zločinu služby kriminální policie a vyšetřování. *Výroční zpráva 2020*. [online]. [cit. 2021-6-30]. Dostupné z: https://www.policie.cz/clanek/web-informacni-servis-zpravodajstvi-vyrocni-zprava-ncoz-2020.aspx?fbclid=IwAR3HaMBspl-4Nf2vIZfQWHkzzEoJ_OWK7g2fECbBoGal7deURIZJ9XKaFzQ

dynamiku lze připodobnit k efektu červené královny[216], kdy každý dílčí krok směrem k větší bezpečnosti v kyberprostoru je následován krokem směřujícím k rozvoji kybernetických hrozeb.

[216] *Efekt červené královny* je matematickým modelem používaným nejčastěji k popisu vztahu evolučního vývoje dvou nebo více druhů, které jsou ve vzájemném konfliktu (predátor a kořist, parazit a hostitel). Ačkoliv dochází k evoluci obou druhů, vzájemná dynamika mezi nimi zůstává stejná. Kontinuální evoluční vývoj jednoho druhu však zabraňuje jeho vyhynutí v důsledku přílišné výhody znepřáteleného druhu. Název pramení z díla spisovatele Lewise Carolla. Zdroj: Efekt červené královny. Wikipedia [online]. [cit. 2021-7-1]. Dostupné z: https://cs.wikipedia.org/wiki/Efekt_%C4%8Derven%C3%A9_kr%C3%A1lovny

3 Trestněprávní aspekty šíření ransomware

Kybernetická kriminalita je dvojí povahy. Jednak kybernetickou kriminalitou rozumíme ty trestné činy, které jsou uskutečnitelné i mimo kyberprostor, informační a komunikační technologie tuto „tradiční kriminalitu v novém kabátě“ pouze usnadňují či jí poskytují odlišnou formu.[217] V tomto případě hovoříme nejčastěji o porušování autorských práv, o různých trestných činech proti lidské důstojnosti v sexuální oblasti, především o nakládání s dětskou pornografií, a o podvodech. Pod pojem kybernetická kriminalita však řadíme i taková jednání, která bez kyberprostoru nejsou myslitelná, jako je šíření nejrůznějších druhů malware, například právě ransomware, či DDoS útoky. Pro účinnou trestněprávní ochranu před kriminálním jednáním činěným v kyperprostoru či jeho prostřednictvím tak bylo nutné přijmout legislativní změny, které by reflektovaly i tyto nové formy kriminálního jednání, které byly před zrodem internetu zcela nemyslitelné a nepředstavitelné. Rovněž bylo třeba u již existujících trestných činů zohlednit nové aspekty, které vznikly v důsledku jejich páchání prostřednictvím kyberprostoru. Řada států tak v důsledku rozmachu kybernetické kriminality přistoupila k legislativním změnám v rámci trestního práva hmotného i procesního, a to buď prostřednictvím dílčích novelizací trestních předpisů, či příjetím nových trestních zákonů specializovaných na kybernetickou kriminalitu (to je případ Velké Británie či Nizozemska).[218]

Na mezinárodní úrovni je v tomto ohledu nejdůležitějším předpisem Úmluva Rady Evropy o kybernetické kriminalitě ze dne 23. 11. 2001, jinak označovaná také jako Budapešťská úmluva. Česká republika pod vlivem této mezinárodní smlouvy přistoupila k zakotvení skutkových podstat trestného činu *neoprávněného přístupu k počítačovému systému a nosiči informací* a trestného činu *opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat* do nového trestního zákoníku z roku 2009. Rovněž došlo k úpravě skutkové podstaty stávajícího trestného činu *poškození a zneužití záznamu na nosiči informací a zásah do vybavení počítače z nedbalosti*. Zákonodárce dále přistoupil k úpravě skutkových podstat trestných činů, které nejsou výlučně počítačovými trestnými činy, například k úpravě skutkové podstaty trestného činu *porušení tajemství dopravovaných zpráv*, *podvodu* či *výroby a jiného nakládání s dětskou pornografií*. Došlo také k dílčím procesním změnám v jinak již poměrně zastaralém trestním řádu,

[217] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ, Ivana a kol. *Kriminologie. 5. aktualizované vydání*. 2019. op. cit. s. 393.
[218] GŘIVNA, Tomáš. *§ 230 Neoprávněný přístup k počítačovému systému a nosiči informací*. In: ŠÁMAL, Pavel a kol. *Trestní zákoník. 2. vydání*. Praha: C. H. Beck, 2012, ISBN 978-80-7400-428-5. s. 2300.

ke komplexním změnám, které by plně zohledňovaly trendy technologického vývoje v kontextu kybernetické kriminality a jejího vyšetřování, dojde však až přijetím připravované rekodifikace trestního práva procesního.[219]

V této části práce si kladu za cíl kvalifikovat šíření ransomware podle českého trestního práva hmotného, a to s ohledem na diferenciaci jednotlivých typů této kybernetické hrozby. Při trestněprávní kvalifikaci ransomware podle jednotlivých ustanovení trestního zákoníku budu předpokládat naplnění obecných znaků trestného činu, tedy věku (§ 25 TZ), příčetnosti (§ 26 TZ) a rozumové a mravní vyspělosti u mladistvého pachatele (§ 5 odst. 1 ZSVM). Pro potřeby této práce vynechám potencionalitu kombinací jednotlivých typů ransomware, kdy například jediný škodlivý kód může zašifrovat soubory uživatele a zároveň jej vydírat zveřejněním některých citlivých informací (tzv. metoda *double extortion*).

Druhou otázkou, na kterou se pokusím v této části práce odpovědět, je otázka, zda je současná právní úprava trestní odpovědnosti za šíření ransomware dostatečná. Analýzu platné právní úpravy doplním vlastními návrhy *de lege ferenda*.

V této části své práce se přidržím toliko trestního práva hmotného, nebudu se zabývat procesněprávními otázkami, ani otázkami jiných právních odvětví, jako je správní právo či právo občanské.

3.1 Trestněprávní kvalifikace ransomware podle platného práva

Jak již bylo uvedeno výše, pod pojem ransomware řadíme hned několik do jisté míry rozdílných kriminálních jednání v kyberprostoru, které mají společného jmenovatele v podobě vyděračského jednání vůči oběti kybernetického útoku. I z tohoto pravidla však existuje výjimka, a to v případě scareware, které jsou sice řazeny odbornou veřejností mezi ransomware, k vydírání oběti při tomto typu útoku však nedochází.

Ve zvláštní části trestního zákoníku nenalezneme jedno konkrétní ustanovení, které by se zaměřovalo na kriminalizaci jednání spočívajícího v šíření ransomware. Jednotlivé skutkové podstaty, které lze tímto jednáním naplnit, jsou rozesety napříč trestním zákoníkem. Jednotlivé typy ransomware útoků mohou přitom být vzájemně natolik rozdílné, že se v rámci zkoumání jednoho jevu bavíme v konkrétních případech o trestných činech se zcela odlišným systematickým

[219] STRAKA, Václav. *Kybernetická kriminalita z trestněprávního pohledu*. Brno, 2020. Diplomová práce. Masarykova univerzita Právnická fakulta. Vedoucí práce doc. JUDr. Josef Kuchta CSc. s. 36.

zařazením. Tzv. počítačové trestné činy, tedy trestné činy podle §§ 230, 231 a 232 TZ, jsou zařazeny do Hlavy V., tedy mezi trestné činy proti majetku. Trestný čin vydírání podle § 175 TZ, řadíme mezi trestné činy proti svobodě do Hlavy II. V kontextu šíření ransomware však můžeme v konkrétních případech uvažovat například také o naplnění skutkových podstat trestných činů přisvojení pravomoci úřadu dle § 328 TZ, který je trestným činem proti pořádku ve věcech veřejných, či obecného ohrožení podle § 272 TZ, které je trestným činem obecně nebezpečným.

Jak již bylo uvedeno, jednotícím prvkem šíření ransomware je jeho vyděračská povaha. V tomto kontextu tak v první řadě budu uvažovat naplnění skutkové podstaty **trestného činu vydírání podle § 175 TZ**. Objektem trestného činu vydírání je svobodné rozhodování člověka v nejširším slova smyslu.[220] Objektivní stránka trestného činu vydírání spočívá v tom, že pachatel jiného násilím, pohrůžkou násilí nebo pohrůžkou jiné těžké újmy nutí, aby něco konal, opominul nebo trpěl. Jedná se o úmyslný trestný čin a pachatelem může být jakákoliv fyzická či právnická osoba, jde tak o subjekt obecný.

Při ransomware útoku pachatel nutí napadenou osobu, aby pod hrozbou ztráty dat, nedostupnosti počítačového systému, zahájení trestního či přestupkového řízení, nebo zveřejnění citlivých údajů odeslala na účet pachatele finanční prostředky. Pachatel tak nutí jiného, aby mu něco dal (latinsky *dare*), tedy aby konal.

Podstatným okamžikem pro posouzení, zda lze šíření ransomware kvalifikovat podle ustanovení § 175 odst. 1 TZ, je úvaha, zda je možné pod *násilí, pohrůžku násilí či pohrůžku jiné těžké újmy* subsumovat výhružky činěné v rámci ransomware útoku. Bezprostřední použití násilí, kterým se dle komentářové literatury rozumí použití fyzické síly k překonání nebo zamezení odporu,[221] je v kyberprostoru nemožné.[222] Pohrůžka násilím sice v kyberprostoru možná je, v takovém případě však nehovoříme o ransomware, ale o běžném vydírání, při kterém informační a komunikační technologie slouží toliko jako komunikační prostředek mezi pachatelem a jeho obětí. V úvahu tak připadá pouze pohrůžka jiné těžké újmy. Aby došlo k naplnění zákonného znaku pohrůžky jiné těžké újmy, je zapotřebí, aby hrozící újma měla určitou intenzitu. Judikatura Nejvyššího soudu k požadované intenzitě uvádí následující:

---

[220] ŠÁMAL, Pavel. *§ 175 Vydírání*. In: ŠÁMAL, Pavel a kol. *Trestní zákoník. 2. vydání*. 2012. op. cit. s. 1750.
[221] ŠÁMAL, Pavel. § 119 *Spáchání trestného činu násilím*. In: ŠÁMAL, Pavel a kol. *Trestní zákoník. 2. vydání*. 2012. op. cit. s. 1305.
[222] Stejně tak je v kyberprostoru velmi obtížně představitelné násilí ve formě uvedení jiného do stavu bezbrannosti lstí nebo jiným obdobným způsobem.

„Pokud jde o pohrůžku jiné těžké újmy, jde o pojem, který není a ani nemůže být jednoznačně definován, neboť zahrnuje velkou škálu okolností, jichž se může taková pohrůžka týkat. V každém případě však jde o neoprávněné jednání pachatele, který hrozí způsobením takových následků, které jsou svou intenzitou obdobné hrozbě spojované s pohrůžkou násilím, tedy mohou u poškozeného vyvolat obavu srovnatelnou např. se situací, kdy je ohroženo zdraví nebo život člověka.“[223]

Komentářová literatura k hodnocení požadované intenzity hrozící újmy oproti výše uvedenému abstraktnímu vymezení přistupuje spíše demonstrativně. Pohrůžka jiné těžké újmy dle ní může spočívat v *„hrozbě způsobení závažné majetkové újmy, vážné újmy na právech, na cti či dobré pověsti, může směřovat k rozvratu manželství nebo rodinného života apod.“*[224] Stejně hovoří i další rozhodnutí Nejvyššího soudu, viz usnesení ze dne 23. 1. 2007 sp. zn. 11 Tdo 1545/2006. Mezi různými typy ransomware se liší typ újmy, kterou pachatel oběti hrozí, ke kvalifikaci konkrétního jednání jako trestného činu vydírání je tak nutné vždy individuálně posoudit, zda se jedná o pohrůžku jiné těžké újmy či nikoliv. Ransomware zpravidla hrozí uživateli trvalou ztrátou dat či učiněním napadeného zařízení neupotřebitelným, zpravidla tak v kontextu útoku ransomware budeme zvažovat, zda bylo možné v důsledku ztráty dat očima poškozeného očekávat závažnou újmu na jeho majetku. V závislosti na typu ransomware však pohrůžka jiné těžké újmy může spočívat i v hrozbě závažné nemajetkové újmy v důsledku ztráty dat, ke které má napadený uživatel citový vztah (např. fotografie, videa, dopisy, jiné osobní dokumenty), v hrozbě poškození dobrého jména či vyzrazení obchodního tajemství či v hrozbě trestním stíháním oběti. Může jít však i o hrozbu ohrožení života a zdraví pacientů v důsledku nedostupnosti zdravotních systémů u nemocnic a jiných zdravotnických zařízení.

V tomto kontextu je pak významné, že při hodnocení intenzity potenciální újmy je třeba vždy nutno přihlížet k osobním poměrům napadené osoby.[225] Může se tak stát, že útoky vůči různým osobám provedené zcela stejným způsobem za použití stejného ransomwaru budou z hlediska naplnění znaků skutkové podstaty trestného činu vydírání posouzeny odlišně.

Podstatný je z hlediska trestněprávního posouzení okamžik, kterým je trestný čin vydírání dokonán. Čin je dokonán již samotným násilným jednáním či pohrůžkou násilí nebo jiné těžké újmy, nevyžaduje se tak dosažení pachatelem zamýšleného účinku.[226] V kontextu útoku

[223] Usnesení NS ve věci sp. zn. 8 Tdo 612/2011 ze dne 15. června 2011.
[224] ŠÁMAL, Pavel. *§ 175 Vydírání*. In: ŠÁMAL, Pavel a kol. *Trestní zákoník. 2. vydání*. 2012. op. cit. s. 1750.
[225] Tamtéž.
[226] Tamtéž.

ransomware je tak pro dokonání trestného činu vydírání určujícím okamžikem zobrazení ransom note uživateli. Z hlediska trestněprávní kvalifikace činu jako dokonaného trestného činu vydírání tak není zapotřebí, aby poškozený pachateli požadovanou částku skutečně zaplatil.

Co se týče možného naplnění znaků kvalifikovaných skutkových podstat, šířením ransomware lze naplnit odstavec 2, a to v případě způsobení značné škody, či s ohledem na skutečnost, zda byl čin spáchán členem organizované osoby či s nejméně dvěma osobami. Odstavec 3 lze naplnit v případě způsobení škody velkého rozsahu, tedy alespoň ve výši 10 000 000,- Kč, což zvláště u cílených ransomware útoků proti společnostem, nemocnicím či kritické infrastruktuře, či v případě mnohosti jednotlivých ransomware útoků, nelze považovat za neobvyklé.

Dalším z hlediska šíření ransomware významným ustanovením je **§ 230 TZ** upravující **trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací**. Ustanovení § 230 zahrnuje hned dvě základní skutkové podstaty, kdy odstavec 1 kriminalizuje již samotné překonání bezpečnostního opatření, kterým pachatel získá neoprávněný přístup k počítačovému systému. Toto ustanovení tak primárně chrání důvěrnost počítačových dat a systémů, jejich dostupnost a integritu chrání až sekundárně.[227] Z hlediska šíření ransomware je tato skutková podstata významná toliko v situaci, kdy dojde k průniku do počítačového systému, avšak z jakéhokoliv důvodu nedojde k použití škodlivého kódu, a tedy nedojde k narušení či poškození dat uživatele ani narušení dostupnosti počítačového systému.

Pokud by došlo k zásahu do dat uživatele či k omezení dostupnosti systému, což lze u útoku ransomware při jeho správné funcionalitě předpokládat, připadala by v úvahu kvalifikace podle odstavce druhého, který na rozdíl od prvního odstavce poskytuje primární ochranu dostupnosti a integritě počítačových dat a systémů. Jednočinný souběh prvního a druhého odstavce je přitom vyloučen, vzhledem ke vztahu subsidiarity prvního odstavce vůči odstavci druhému.[228] Druhý odstavec zahrnuje řadu poměrně kazuisticky vyjádřených jednání, z hlediska kvalifikace šíření ransomware je významné zejména ustanovení § 230 odst. 2 písm. b) TZ, které kriminalizuje jednání, kdy pachatel „*získá přístup k počítačovému systému nebo k nosiči informací a data uložená v počítačovém sytému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými*“.

---

[227] GŘIVNA, Tomáš. *§ 230 Neoprávněný přístup k počítačovému systému a nosiči informací*. In: ŠÁMAL, P. a kol. *Trestní zákoník. 2. vydání*. 2012, op. cit. s. 2300.
[228] KRUPIČKA, Jiří. *Trestněprávní a kriminologické aspekty internetové kriminality*. 2012. op. cit. s. 89.

V úvahu připadá i naplnění znaků kvalifikované skutkové podstaty podle odstavce 3, kdy kvalifikačními znaky jsou alternativně buď úmysl způsobit jinému škodu nebo jinou újmu, či získat sobě nebo jinému neoprávněný prospěch, což je u ransomware typické, nebo úmysl omezit funkčnost počítačového systému nebo jiného zařízení pro zpracování dat, což je naplněno u locker-ransomware útoků. Podle závažnosti konkrétního útoku a výše způsobené škody, či dle výše získaného výkupného, pak můžeme uvažovat i naplnění kvalifikovaných skutkových podstat podle odstavců 4 a 5. Opět lze obecně říci, že u ransomware útoků nezřídka dochází k prolomení hranice škody velkého rozsahu, což kvalifikaci takovéhoto činu posunuje do pátého odstavce.

Obvyklou trestněprávní kvalifikací ransomware nehledě na typ použitého ransomware (kromě již zmiňovaného scareware) tak může být trestný čin vydírání podle § 175 odst. 1 TZ (případně dle odstavců 2 a 3) v jednočinném souběhu s trestným činem neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 2 písm. b), odst. 3 písm. a) TZ, případně i odstavce 4 a 5 podle rozsahu způsobené škody či hodnoty získaného prospěchu.

Ve zvláštních případech, jako jsou útoky na nemocniční zařízení či na kritickou infrastrukturu, můžeme uvažovat i o naplnění znaků trestného činu obecného ohrožení dle § 272 TZ, poškození a ohrožení provozu obecně prospěšného zařízení z nedbalosti dle § 277 TZ či teroristického útoku dle § 311 TZ.[229]

3.1.1 Šifrovací ransomware

Podstatným aspektem varianty šifrovacího ransomware je skutečnost, že útočník hrozí napadenému uživateli ztrátou dat. Z hlediska trestněprávního posouzení jako trestného činu vydírání je zásadní otázkou, zda je možné hrozbu ztráty dat uživatele subsumovat pod zákonný znak *pohrůžky jiné těžké újmy*. V tomto smyslu je případná kvalifikace šíření šifrovacího ransomware jako trestného činu vydírání závislá na celé řadě faktorů a je nutné hodnotit individuální okolnosti každého jednotlivého případu. Významnými faktory jsou především povaha napadených dat a jejich význam pro poškozeného. Počítačové systémy mohou například obsahovat pouze data bez ekonomického či osobního významu, jejichž ztrátu uživatel vnímá jako minimální újmu či ji jako újmu nevnímá vůbec, pak by se o pohrůžku jiné těžko újmy zjevně nejednalo. Ztráta dat s ekonomickou hodnotou však, s ohledem na výši případné majetkové škody, pohrůžkou jiné těžké újmy být může. Stejně tak jí může být i ztráta dat s významnou nemajetkovou hodnotou,

[229] Ustanovení § 311 odst. 1 písm. e) TZ se zaměřuje konkrétně na projevy kyberterorismu.

ohled v individuálních případech můžeme brát například na případný dopad ztráty osobních dat na rodinný život poškozeného. [230]

Při úvahách o možné kvalifikaci šifrovacího ransomware jako trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 2 TZ je třeba subsumovat zašifrování souborů pod jeden z alternativních znaků obsažených v písmenech a) až d). Zašifrováním dat sice nedojde k jejich smazání, data zůstávají zachována, ale bez následné dešifrace nemají pro uživatele žádnou hodnotu, jelikož jsou nepoužitelná ve smyslu svého původního účelu. Podle komentářové literatury se tak jedná o učinění dat neupotřebitelnými, což odpovídá písmenu b). [231]

3.1.2 Locker-ransomware

Prvně opět ke kvalifikaci činu jako TČ vydírání. Při rozhodování, zda může být výhružka odepření přístupu k zařízení a k datům v něm obsažených pohrůžkou jiné těžké újmy, je i v tomto případě nutné posuzovat konkrétní okolnosti každého jednotlivého případu. Je nutné posuzovat zejména význam blokovaného zařízení a možné důsledky jeho blokování, stejně tak i význam a povahu dat v zařízení obsažených, podobně jako u šifrovacího ransomware. Vzhledem ke skutečnosti, že velkou spoustu méně technicky vyspělých locker-ransomware lze za použití určité míry technických schopností a dovedností obejít, bude při trestněprávní kvalifikaci tohoto činu významným faktorem také technická znalost poškozeného, kdy výhružka omezením funcionality zařízení nemusí být vůbec způsobilá vyvolat v napadeném uživateli obavu, že k omezení zařízení dojde. Čin by tak byl trestný jako pokus trestného činu vydírání dle § 21 odst. 1 TZ ve spojení s § 175 odst. 1 TZ.

Co se týče kvalifikace locker-ransomware podle § 230 odst. 2 TZ, stejně jako v případě šifrovacího ransomware přichází v úvahu kvalifikace podle písmene b), jelikož při znepřístupnění nosiče dat či počítačového systému, který obsahuje data, jsou tato data učiněna neupotřebitelnými. Pokud zablokované zařízení neobsahuje uživatelsky významná data, či pokud nedojde k učinění takových dat neupotřebitelnými, subsidiárně může dojít k naplnění znaku obsaženém v písmenu d), které kriminalizuje další zásahy do programového nebo technického vybavení zařízení nezmíněné v písmenech a) až c). Významné je rovněž naplnění znaku kvalifikované skutkové podstaty dle odstavce třetího, písmene b), tedy znaku úmyslného neoprávněného omezení

[230] JOHANOVSKÝ, T. *Kriminologické a trestněprávní aspekty fenoménu ransomware*. 2018. op. cit. s. 43.
[231] GŘIVNA, Tomáš. *§ 230 Neoprávněný přístup k počítačovému systému a nosiči informací*. In: ŠÁMAL, P. a kol. *Trestní zákoník. 2. vydání*. 2012, op. cit. s. 2300.

funkčnosti systému. Právě omezení funkčnosti systému je hlavním mechanismem fungování drtivé většiny locker-ransomware.

Pokud se bavíme o omezení funkčnosti zařízení IoT, jakou jsou například prvky chytré domácnosti, zde se může jevit jako problém subsumpce takového typu zařízení pod zákonný pojem „*počítačový systém*“. Dle komentáře se počítačovým systémem rozumí: *„jakékoli zařízení nebo skupina vzájemně propojených nebo souvisejících zařízení, z nichž jedno nebo více provádí na základě programu automatické zpracování dat. Počítačovým systémem je tedy zařízení sestávající z technického (hardware) a programového (software) vybavení, které je určené k automatickému zpracování digitálních dat. Automatickým zpracováním se rozumí zpracování bez přímého lidského zásahu. Zpracování dat znamená, že na data se v počítačovém systému působí prováděním počítačového programu.“*[232]

Je otázkou, zda prvky IoT výše uvedenou definici naplňují. Lze říci, že každé zařízení IoT má svou technickou i programovou část a do určité míry je součástí jeho funkcionality zpracování dat. Nelze však bez dalšího říci, že každé zařízení s připojením k internetu je ke zpracování dat primárně určeno. Kupříkladu lze uvést chytrou ledničku, která sbírá data o množství a druhu uskladněných potravin a tato data dále prostřednictvím počítačového programu zpracovává. Na základě zpracování těchto dat pak například upozorní uživatele na nedostatek určité konkrétní potraviny či dokonce chybějící potraviny automaticky nakoupí přes e-shop. Účelem tohoto zařízení je však stále primárně uchovávat potraviny v chladné teplotě, notifikace uživatele a nákup surovin jsou až funkce sekundární. Stejně tak lze hovořit o automobilech, kdy je dnes již zcela běžně, že část jejich funkcionality spojena s internetovým připojením a zpracováním dat. Zdá se však obtížně obhajitelným subsumovat automobil pod pojem počítačový systém ve smyslu ustanovení § 230 TZ. Dle mého názoru tak u locker-ransomware útoků proti jednotlivým druhům IoT zařízení, jejichž primárním účelem není zpracování a uchování dat, lze uvažovat spíše o naplnění znaků skutkové podstaty trestného činu poškození cizí věci podle § 228 odst. 1 TZ.

3.1.3 Doxware

Pro posouzení doxware, jehož principem je vyhrožování oběti zveřejněním citlivých dat, jako trestný čin vydírání je opět třeba individuálně posoudit, zda činěné výhružky naplňují znak pohrůžky jiné těžké újmy. V tomto případě je zřejmé, že nejvýznamějším faktorem při posuzování

[232] GŘIVNA, Tomáš. *§ 230 Neoprávněný přístup k počítačovému systému a nosiči informací*. In: ŠÁMAL, P. a kol. *Trestní zákoník. 2. vydání*. 2012, op. cit. s. 2300.

naplnění zákonného znaku pohrůžky jiné těžké újmy bude povaha napadených dat a případný negativní důsledek jejich zveřejnění pro poškozeného. Jelikož doxware nejčastěji cílí na podnikatelské subjekty, bude se jednat především o data spojená s obchodní činností poškozeného. Zpravidla se bude jednat o osobní údaje klientů a zaměstnanců poškozeného, data, která jsou součástí obchodního tajemství, a ekonomické údaje o poškozeném. Ohroženým zájmem poškozeného je v tomto případě zpravidla dobrá pověst v očích klientů a jeho ekonomická konkurenceschopnost. I v tomto případě je nutné vyhodnocovat každý konkrétní případ, ale je pravděpodobné, že v případě doxware útoků na podnikatelské subjekty k naplnění znaku pohrůžky jiné těžké újmy dojde.

Co se týče kvalifikace doxware podle § 230 odst. 2 TZ, v tomto případě lze zvažovat aplikaci písmene a), které obsahuje znak neoprávněného užití dat uložených v počítačovém systému či na nosiči informací, avšak pouze za předpokladu, že skutečně dojde ke zveřejnění citlivých dat útočníkem. V jiném případě lze aplikovat písmeno d), kdy již samotnou infikací zařízení ransomware lze považovat za jiný zásah do programového vybavení počítačového systému.

V případě zveřejnění citlivé korespondence poškozeného uvnitř společnosti či se třetími osobami je namístě kvalifikace takového skutku jako trestný čin porušení tajemství dopravovaných zpráv dle § 182 odst. 2 TZ, který je samostatnou skutkovou podstatou postihující jednání, které spočívá v prozrazení či zneužití tajemství dopravovaných zpráv v úmyslu způsobit jinému škodu či v úmyslu získat sobě nebo jinému neoprávněný prospěch. Pokud se jedná o jiný typ listin a dokumentů uchovávaných v soukromí, než jsou dopravované zprávy, uplatnil by se trestný čin porušení tajemství listin a jiných dokumentů uchovávaných v soukromí podle § 183 odst. 1 TZ. V případě zveřejnění obchodního tajemství může být čin kvalifikován jako TČ porušení předpisů o pravidlech hospodářské soutěže podle ustanovení § 248 odst. 1 písm. h) TZ, a to za předpokladu, že se tohoto činu pachatel dopustil při účasti v hospodářské soutěži, a že tím bude soutěžiteli nebo spotřebitelům způsobena újma ve větším rozsahu či pokud tím pachatel opatří sobě nebo jinému ve větším rozsahu neoprávněné výhody.

3.1.4 Policejní virus

V trestněprávní rovině je policejní virus významný kvůli skutečnosti, že se útočník pro posílení psychologického účinku na poškozeného vydává za orgán veřejné moci, nejčastěji právě policie. Zpravidla pak poškozenému tento typ ransomware hrozí trestním stíháním z důvodu tvrzené přítomnosti nelegálního obsahu v zařízení poškozeného (jako jsou pirátské kopie

autorských děl, nelegální verze softwaru či pornografie), přičemž hrozbu trestního stíhání lze odvrátit jednorázovou platbou na bitcoinový účet útočníka. Z pohledu naplnění znaků skutkové podstaty trestného činu vydírání tak budeme zkoumat, zda je hrozba trestním stíháním pohrůžkou jiné těžké újmy či nikoliv. Dle judikatury NS[233] může být hrozba trestním stíháním pohrůžkou jiné těžké újmy ve smyslu TČ vydírání, a to nezávisle na skutečnosti, zda se poškozený trestné činnosti, v jejímž důsledku mu trestní stíhání hrozí, dopustil či nikoliv. V tomto kontextu však bude významné, zda poškozený hrozbu trestním stíháním činěnou prostřednictvím policejního viru jako hrozící újmu vnímal, tedy zda útočníkovi skutečně uvěřil.

Policejní virus zpravidla funguje jako locker-ransomware, a to v tom smyslu, že omezí přístup uživatele k zařízení, pro otázku kvalifikace dle § 230 odst. 2 TZ tak odkazuji na rozbor uvedený v bodě 3.1.2.

V případě policejního viru je třeba zkoumat rovněž potencialitu naplnění znaků skutkové podstaty trestného činu přisvojení pravomoci úřadu podle ustanovení § 328 TZ. Útočníci totiž zpravidla prezentují požadovanou platbu jako veřejnoprávní sankci za nelegální jednání poškozeného. Ustanovení § 328 TZ obsahuje dvě alternativy, přičemž alinea první postihuje *vykonávání* úkonů, které jsou vyhrazeny orgánům veřejné moci, zatímco alinea druhá postihuje *vykonání* úkonu, který může být vykonán jen z moci úřední orgánů veřejné moci.[234] Typickým příkladem trestného činu přisvojení pravomoci úřadu je vydávání se za příslušníka Policie ČR vykonávajícím silniční kontrolu a následné vybírání „pokut".[235] Pokud se útočník vydává za útvar Policie ČR při výběru správních sankcí, bylo by možné subsumovat i jednání spočívající v šíření policejního viru pod jednu ze dvou skutkových podstat obsažených v ustanovení § 328 TZ. Dle mého názoru pak není zásadním problémem fakt, že způsob výběru „pokut" zjevně neodpovídá skutečným procesním postupům příslušného orgánu veřejné moci, tedy skutečnost, že Policie ČR při své činnosti na úseku přestupků ani v rámci trestního řízení neblokuje počítače a nerozesílá vymahačské zprávy prostřednictvím internetu. Zásadním aspektem věci je samotná podstata tohoto jednání, tedy skutečnost, že se útočník za orgán veřejné moci při výkonu činnosti vyhrazené tomuto orgánu vydává. Co se týče jednočinného souběhu tohoto trestného činu s trestným činem vydírání, uvádím, že ten není vyloučen, a to i s přihlédnutím k judikatuře trestních soudů[236].

---

[233] Rozsudek NS sp. zn. 6 Tz 12/81 ze dne 8. 4. 1981.
[234] JELÍNEK, Jiří. *Trestní právo hmotné: obecná část, zvláštní část. 6. aktualizované a doplněné vydání*. Praha: Leges, 2017. ISBN 978-80-7502-236-3. s. 832 – 833.
[235] Jako příklad těchto kauz odkazuji na skutkový stav ve věcech sp. zn. 6 Tdo 1480/2014 či sp. zn. 7 Tdo 650/2016.
[236] Viz usnesení NS č. j. 6 Tdo 1480/2014-20 ze dne 24. 2. 2015.

U policejního viru připadá v úvahu také trestněprávní kvalifikace jako TČ podvodu podle § 209 odst. 1 TZ, v této věci odkazuji na následující podkapitolu 3.1.5. Případný jednočinný souběh TČ podvodu a TČ přisvojení pravomoci úřadu pak dle mého názoru není vyloučen.

3.1.5 Scareware

Jak již bylo opakovaně uvedeno, při útoku scareware nedochází k naplnění skutkové podstaty trestného činu vydírání. Nemusí docházet dokonce ani k naplnění znaků skutkové podstaty trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací, vzhledem ke skutečnosti, že mnohé scareware fungují jako vyskakovací okna, která se aktivují již při navštívení určitých internetových stránek, nemusí tak vůbec dojít k získání přístupu k počítačovému systému poškozeného. Pokud se v daném případě o překonání bezpečnostního opatření a získání přístupu do počítačového systému jedná, budeme zřejmě uvažovat o kvalifikaci podle § 230 odst. 2 písm. d) TZ.

Zásadním bodem u tohoto typu ransomware je však jeho trestněprávní kvalifikace jako TČ podvodu dle ustanovení § 209 odst. 1 TZ, vzhledem ke skutečnosti, že útočník uvádí poškozeného v omyl tím, že mu prostřednictvím vyskakovacího okna či jiným způsobem sdělí nepravdivou informaci, že došlo k infikaci jeho zařízení škodlivým softwarem a pro jeho odstranění je třeba zaplatit příslušnou částku. Pro naplnění znaků základní skutkové podstaty tohoto trestného činu je třeba způsobit na cizím majetku škodu nikoliv nepatrnou, tedy alespoň v hodnotě 10 000,- Kč, což je vzhledem k obvyklé mnohosti jednotlivých útoků v rámci pokračování jediného trestného činu často naplněno. Na rozdíl od většiny jiných typů ransomware, v případě tohoto typu útoku dojde k dokonání ve smyslu trestného činu podvodu až v okamžiku zaplacení požadované částky poškozeným. Do té doby lze hovořit o pokusu trestného činu podvodu či o přípravě trestného činu podvodu, která je v případě kvalifikované skutkové podstaty podle odstavce 5 rovněž trestná.

Dle Smejkala je přitom v souladu s judikaturou možnost jednočinného souběhu trestného činu podvodu s trestným činem neoprávněného přístupu k počítačovému systému a nosiči informací. Odkazuje přitom na usnesení Nejvyššího soudu ze dne 16. 3. 2006 ve věci sp. zn. 6 Tdo 289/2006.[237]

[237] SMEJKAL, Vladimír. *Kybernetická kriminalita. 2. rozšířené a aktualizované vydání*. 2018. op. cit. s. 200.

3.1.6 Ransomware-as-a-service

Problematiku RaaS v souvislostech s její trestněprávní kvalifikací je nutné rozdělit do dvou kategorií. První kategorií jsou služby spočívající nejen ve vytvoření škodlivého kódu, ale rovněž v jeho distribuci, případně i ve výběru výkupného. V tomto případě při posuzování, jaké skutkové podstaty trestných činů naplnil hacker poskytující RaaS služby, nelze než odkázat na výše uvedené kvalifikace dle jednotlivých typů ransomware. Co se týče trestní odpovědnosti objednatele těchto služeb, jednalo by se zpravidla o účastenství na trestném činu hlavního pachatele, tedy konkrétního RaaS hackera, ve formě návodu dle § 24 odst. 1 b) TZ. Návodcem je ten, kdo v jiném úmyslně vzbudí rozhodnutí spáchat trestný čin. Zákon přitom nestanoví konkrétní prostředky návodu, ty mohou být jakékoliv.[238] Návod je možný mimo jiné i ujednáním za mzdu[239], což je případ RaaS. Dle míry spoluúčasti objednatele RaaS služeb by však bylo teoreticky možné uvažovat i o spolupachatelství dle § 23 TZ.

Druhou kategorií je pak pouhé vytvoření škodlivého kódu na objednávku, přičemž o šíření takto zakoupeného škodlivého kódu se postará samotný objednatel. Objednatel, který by byl v daném případě tím, kdo fakticky vykoná průnik do cizího zařízení a uživatele tohoto zařízení vydírá, by byl trestně odpovědný stejně, jako by použil vlastnoručně vytvořený škodlivý kód. Na jeho trestněprávní odpovědnosti by se tak v důsledku použití na zakázku vytvořeného ransomware nic nezměnilo. Co se týče tvůrce škodlivého kódu, zde přichází v úvahu trestněprávní kvalifikace podle ustanovení § 231 odst. 1 TZ, tedy trestného činu opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat. Toto ustanovení kriminalizuje již samotnou výrobu, uvedení do oběhu, dovoz, vývoz, provezení, nabídku, zprostředkování, prodej nebo jiné zpřístupnění, opatření a přechovávání prostředků umožňujících neoprávněný přístup do počítačového systému či do sítě elektronických komunikací, a to v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv či trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací.[240] Vůči těmto dvěma trestným činům je tak ustanovení § 231 odst. 1 TZ předčasně dokonaným trestným činem. Nabídku, výrobu, prodej a další nakládání s ransomware programy, respektive s exploit kity, které slouží ke zneužití zranitelnosti

[238] JELÍNEK, Jiří. *Trestní právo hmotné: obecná část, zvláštní část. 6. aktualizované a doplněné vydání*. 2017. op. cit. s. 317.
[239] Tamtéž.
[240] Nedochází tak ke kriminalizaci jednání, které spočívá ve tvorbě škodlivých programů, exploit kitů a dalších metod, které nejsou tvořeny s úmyslem neoprávněně pronikat do cizích zařízení, ale za účelem zdokonalování bezpečnostních systémů a hledání slabin, což je předmětem white hat hackingu.

počítačového systému za účelem vniknutí do systému a aktivace ransomware, či s dalšími souvisejícími programy a metodami tak lze subsumovat pod toto ustanovení.

3.2 Hodnocení platné právní úpravy a návrhy de lege ferenda

Současnou úpravu trestněprávní odpovědnosti za šíření ransomware nelze dle mého názoru považovat za ideální. Odbornou veřejností bývá často kritizována především úprava počítačových trestných činů v ustanoveních §§ 230 až 232 TZ. Dle Jelínka jsou skutkové podstaty obsažené v těchto třech ustanoveních příliš kazuistické a zákonodárce jako by rezignoval na abstraktní právní jazyk.[241] Kazuističnost uvedeným ustanovením vytkl také Krupička.[242] Z přílišné komplexnosti a kazuističnosti těchto ustanovení rovněž vyplývají některé legislativně technické nepřesnosti, které ještě více komplikují právní výklad a aplikaci těchto ustanovení v konkrétních případech. Problém může nastat již u výkladu pojmů *počítač* a *počítačový systém* a v jejich odlišování, k diferenciaci těchto dvou pojmů přistoupil zákonodárce v ustanovení § 230 odst. 2 písm. d) TZ:

*„d) neoprávněně vloží data do **počítačového systému** nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení **počítače** nebo jiného technického zařízení pro zpracování dat“.*

Podle komentářové literatury je pojem počítačový systém pojmem širším a zahrnuje jakékoli zařízení nebo skupinu vzájemně propojených nebo souvisejících zařízení, z nichž jedno nebo více provádí na základě programu automatické zpracování dat.[243] Výklad komentáře tak odpovídá definici pojmu *počítačový systém* dle čl. 1 Úmluvy o kybernetické kriminalitě. K pojmu *počítač* komentář uvádí, že je někdy používán jako synonymum pojmu počítačový systém, avšak rozdíl spočívá ve skutečnosti, že počítačový systém zahrnuje i síťově připojená zařízení, která pojmově nesplňují atributy počítače.[244] Smejkal s uvedeným významovým odlišením pojmu počítač od pojmu počítačový systém, kdy počítačový systém kromě počítače zahrnuje také periferní zařízení, souhlasí, avšak v kontextu skutkové podstaty trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací dle ustanovení § 230 TZ by volil přidržení se

[241] JELÍNEK, Jiří. *Trestní právo hmotné: obecná část, zvláštní část. 6. aktualizované a doplněné vydání*. 2017. op. cit. s. 673.
[242] KRUPIČKA, Jiří. *Trestněprávní a kriminologické aspekty internetové kriminality*. 2012. op. cit. s. 83.
[243] GŘIVNA, Tomáš. *§ 230 Neoprávněný přístup k počítačovému systému a nosiči informací*. In: ŠÁMAL, Pavel a kol. *Trestní zákoník. 2. vydání.* 2012, op. cit. s. 2300.
[244] Tamtéž.

toliko pojmu počítačový systém.[245] Tento názor podporuji a doplňuji, že nesystematičnost používání těchto dvou pojmů se projevuje i v dalších ustanoveních trestního zákoníku, jako jsou ustanovení §§ 120, 264 a 267 TZ.

Za chybu legislativní techniky by bylo dále možné ve shodě s Krupičkou označit výčet možných způsobů nakládání s daty podle § 230 odst. 2 písm. b) TZ, přičemž by bylo zcela dostatečným jejich zobecnění pojmem „změna".[246]

Mohlo by se zdát, že se jedná o nedostatky, které nejsou zásadními problémy právní úpravy kybernetické kriminality. Jednoznačně lze souhlasit s názorem, že uvedené výkladové problémy lze vyřešit i bez legislativního zásahu do platné právní úpravy, a to prostřednictvím výkladové praxe soudů. Obětí komplexní, kazuistické a příliš doslovné úpravy počítačových trestných činů je však ve výsledku samotná srozumitelnost právní normy, což je vzhledem k zásadě *nullum crimen sine lege certa*, tedy k požadavku na určitost, jasnost a srozumitelnost trestněprávní normy do takové míry, aby adresát trestněprávní normy neměl pochybnosti o tom, kdy a za jakých podmínek se jeho chování stává trestným[247], jevem nežádoucím.

Druhým problémem, který přílišná kazuističnost skutkových podstat počítačových trestných činů přináší, je skutečnost, že v případě rozsáhlého výčtu jednotlivých jednání může dojít k „propadnutí" některých společensky škodlivých jednání souvisejících s počítačovými systémy sítem trestní odpovědnosti. To ostatně uvádí i Smejkal na příkladu *jiného zásahu* (ve smyslu ustanovení § 230 odst. 2 písm. d) TZ) na periferní zařízení, jako je například externí jednotka CD/DVD, které samo o sobě není počítačem, kdy si dle něj lze představit obhajobu založenou na tvrzení, že nedošlo k naplnění zákonného znaku skutkové podstaty, jelikož se nejednalo o počítač ani o jiné technické zařízení pro zpracování dat, jelikož ke zpracování dat dochází až v hlavní výpočetní jednotce počítače.[248] Při dostatečně zobecněné skutkové podstatě se lze těmto problémům vyhnout daleko snáze.

K dobru českého zákonodárce lze na druhou stranu uvést, že otázka vhodné úpravy kybernetické kriminality v rámci trestního práva hmotného není z otázek nejjednodušších. Zákonodárce by měl na jednu stranu usilovat o dostatečnou obecnost při vymezování skutkových

---

[245] SMEJKAL, Vladimír. *Kybernetická kriminalita. 2. rozšířené a aktualizované vydání*. 2018. op. cit. s. 571.
[246] KRUPIČKA, Jiří. *Trestněprávní a kriminologické aspekty internetové kriminality*. 2012. op. cit. s. 134.
[247] JELÍNEK, Jiří. *Trestní právo hmotné: obecná část, zvláštní část. 6. aktualizované a doplněné vydání*. 2017. op. cit. s. 30.
[248] SMEJKAL, Vladimír. *Kybernetická kriminalita. 2. rozšířené a aktualizované vydání*. 2018. op. cit. s. 571.

podstat jednotlivých trestných činů obsažených ve zvláštní části trestního zákoníku, na druhou stranu však musí být zohledněna zvláštní povaha trestných činů spáchaných v kyberprostoru, vzhledem ke skutečnosti, že se v případě kybernetických trestných činů můžeme bavit o zcela odlišné společenské škodlivosti, než u jejich ekvivalentů ve fyzickém světě, či o zcela nových kriminálních jednáních. Rovněž hovoříme o odlišné množině pachatelů i obětí, jak již bylo zmíněno v kriminologické části této práce. Aby tak byla zachována ochranná funkce trestního práva, musí na tyto odlišnosti zákonodárce určitým způsobem reagovat.

Co se týče návrhů *de lege ferenda*, domnívám se, že vzhledem k aktuálnímu vývoji šíření ransomware a zvyšující se společenské nebezpečnosti tohoto jevu, je potřebné zohlednění existence ransomware jako specifického způsobu vydírání v trestním právu hmotném. Potřebné je nejen přísnější trestání tohoto typu chování oproti běžnému vydírání, ale také zakotvení trestnosti přípravy šíření ransomware i bez nutnosti dosáhnout na vznik škody velkého rozsahu. Již samotná příprava šíření ransomware může vykazovat znaky vysoké společenské nebezpečnosti, může se jednat o spolčování hackerů a zločineckých skupin před provedením útoku, opatřování a tvorbu softwarových i jiných prostředků k provedení či usnadnění průniku do počítačového systému (v tomto konkrétním případě by bylo možné dovodit trestnost i nyní podle ustanovení § 231 TZ), ale také o sběr informací o budoucí oběti v případě přípravy sofistikovaného kybernetického útoku. Pro efektivní ochranu právem chráněných zájmů by tak dle mého názoru měla být trestná již tato činnost.

Příprava je dle ustanovení § 20 odst. 1 TZ trestná, pokud to zákon u příslušného trestného činu stanoví, a to pouze u zvlášť závažných zločinů. Zvlášť závažnými zločiny jsou podle § 14 odst. 3 TZ ty úmyslné trestné činy, u kterých zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně 10 let.

Současná úprava umožňuje trestání přípravy TČ vydírání jen v případě způsobení těžké újmy na zdraví, škody velkého rozsahu či v souvislosti se spácháním teroristického trestného činu, s financováním terorismu nebo s vyhrožováním teroristickým trestným činem. V případě ransomware tak bude významným faktorem právě způsobení škody velkého rozsahu, která dle aktuálního znění TZ činí 10 000 000,- Kč. Z pohledu dokazování by však v případě nedokonaného činu šíření ransomware bylo zpravidla velice obtížné prokázat, že by v případě dokonání ransomware došlo ke způsobení škody alespoň v této výši. Před provedením samotného útoku je téměř nemožné určit, jakou škodu by daný útok způsobil. Nemusí být zřejmý počet cílových zařízení, hodnota napadených souborů ani následky pro oběť takového případného útoku. Kybernetický útok navíc nemusí vůbec proniknout bezpečnostním systémem oběti.

Dalo by se namítnout, že je příprava ransomware trestná podle ustanovení § 231 odst. 1 TZ jako opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat, jak bylo ostatně uvedeno již dříve v této práci. Na tomto místě je však nutné podotknout, že dané ustanovení kriminalizuje pouze některé formy přípravy šíření ransomware, a to konkrétně různé formy dispozice se samotným škodlivým kódem určeným k průniku do počítačového systému oběti, jako je jeho výroba, nabídka, přechovávání, prodej, atd. Jiné formy přípravy, jako je organizování, návod, pomoc, spolčení k provedení útoku a další, by tak podle současné úpravy byly beztrestné.

Po ukotvení trestnosti přípravy u kybernetických útoků volá i Kolouch. Ten jde směrem navýšení sankcí u trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 TZ a přidání nového odstavce, který by zakotvil trestnost přípravy u tohoto trestného činu.[249] V případě jeho návrhu by však příprava byla trestná pouze při naplnění znaků kvalifikované skutkové podstaty dle současného odst. 4, kdy by bylo opět třeba zkoumat předpokládaný účinek, který by nastal v případě dokonání trestného činu, či by se muselo jednat o činnost člena organizované skupiny. I přesto lze tento návrh podpořit, a to zejména z hlediska zakotvení přísnějších sankcí i pro jiné typy kybernetických útoků, než je ransomware.

Co se týče mého konkrétního návrhu na změnu právní úpravy, nedomnívám se, že je vhodným způsobem vytvoření zcela nové zvláštní základní skutkové podstaty trestného činu, která by odpovídala pojmovým znakům ransomware. Vzhledem ke stále rostoucímu množství typů kybernetických útoků a neustálému vývoji kybernetických hrozeb by hrozilo zahlcení zvláštní části trestního zákoníku různými typy nových kybernetických trestných činů a došlo by k prohloubení výše uvedených problémů s příliš kazuistickou právní úpravou počítačových trestných činů.

Možným řešením by bylo zakotvení nového znaku kvalifikované skutkové podstaty v rámci ustanovení § 175 TZ, trestného činu vydírání, který by odpovídal definičním znakům ransomware. Toto řešení by odpovídalo i celkové koncepci trestního zákoníku, kdy základní skutkové podstaty zpravidla vymezují skutkové podstaty co možná nejobecnějším způsobem, přičemž konkrétní a často až specifické znaky zohledňující zvýšenou společenskou závažnost činu jsou obsaženy až v jednotlivých kvalifikovaných skutkových podstatách.

---

[249] KOLOUCH, Jan. *CyberCrime*. 2016. op. cit. s. 464.

Obtížnou legislativně technickou otázkou by pak byla textace takovéhoto ustanovení. Jednou z možností by bylo stanovení znaku kvalifikované skutkové podstaty spočívající v pohrůžce ztrátou dat nebo zablokováním počítačového systému. Tento způsob by ovšem plně nezohledňoval povahu ransomware, kdy se jedná o typ technologického nástroje. Zcela teoreticky by tak daný znak mohl být naplněn i ústním vyhrožováním smazáním dat nebo zablokováním počítače, kdy by zcela paradoxně byl daný čin kvalifikován přísněji než v případě použití násilí či v případě pohrůžky násilím.

Další možností, která by mohla připadat v úvahu, a která by zohledňovala technologickou povahu ransomware, by bylo stanovení znaku kvalifikované skutkové podstaty spočívajícím ve spáchání činu prostřednictvím sítí informačních a komunikačních technologií. Ani tato úprava by však nebyla vhodná, jelikož prostřednictvím sítí informačních a komunikačních technologií může docházet ke zcela standardnímu vydírání, a to například prostřednictvím e-mailových zpráv, hovorů a sociálních sítí. Od ústního vyhrožování či písemných dopisů by se tak tato jednání lišila pouze ve formě, prostřednictvím které pachatel oběti hrozí.

Dané ustanovení by tak mělo reflektovat technologickou povahu ransomware a také skutečnost, že ransomware jakožto technologický prostředek, prostřednictvím kterého je oběť vydírána, slouží k zašifrování nebo k jinému pozměnění (či dokonce ke zničení) dat či k omezení přístupu k počítačovému systému, respektive k jeho poškození, zničení či učinění neupotřebitelným. Navrhuji tak následující znění znaku kvalifikované skutkové podstaty k trestnému činu vydírání podle § 175 TZ:

„spáchá-li takový čin prostřednictvím zařízení nebo jeho součásti, postupu, nástroje nebo jakéhokoliv jiného prostředku, včetně počítačového programu, sloužícímu ke zničení, poškození nebo omezení počítačového systému nebo k učinění počítačového systému neupotřebitelným, nebo ke zničení, poškození nebo změně dat uložených v počítačovém systému nebo na nosiči informací nebo k učinění těchto dat neupotřebitelnými“

Jak je patrné z výše uvedené textace, i přes vytýkané nedostatky zákonné úpravy počítačových trestných činů dle §§ 230 až 231 TZ jsem zachoval obdobnou terminologii, tvorba terminologie zcela nové by právní úpravu ještě komplikovala a činila ji o to méně srozumitelnou.

Otázkou zůstává, zda navrhovanou úpravu podřadit pod odstavec 2, který stanovuje trestní sazbu trestu odnětí svobody v délce dvě léta až osm let, či pod odstavec 3, kde činí trestní sazba pět až dvanáct let, či vytvořit zcela nový odstavec s vlastní trestní sazbou. Z pohledu zakotvení trestnosti přípravy by se jako vhodné řešení jevilo zařazení mého návrhu jako písmena d) pod

odstavec 3., kde je horní hranice trestní sazby 12 let. Problémem by však v tomto případě byla příliš vysoká dolní hranice trestní sazby, která v tomto případě činí 5 let, a to vzhledem ke skutečnosti, že útoky ransomware zahrnují poměrně širokou škálu jednání s různým stupněm společenské nebezpečnosti. Hrozilo by tak nepřiměřeně přísné trestání pachatelů ojedinělých útoků nikoliv sofistikované povahy, jako jsou například již zmiňovaní script kiddies.

Vhodným řešením by bylo dle mého názoru vytvoření nového odstavce 3, který by obsahoval mnou navrhovanou úpravu. Co se týče navrhované trestní sazby, mělo by jít o dostatečně široký rámec, aby bylo možné zohlednit různě vysokou společenskou nebezpečnost šíření ransomware. Svou závažností je ransomware někde na pomezí odstavce 2 a současného odstavce 3, navrhoval bych tak trestní sazbu ve výši tři až deset let. Navrhovaný odstavec 3 by tak zněl následovně:

„(3) Odnětím svobody na tři léta až deset let bude pachatel potrestán, spáchá-li takový čin prostřednictvím zařízení nebo jeho součásti, postupu, nástroje nebo jakéhokoliv jiného prostředku, včetně počítačového programu, sloužícímu ke zničení, poškození nebo omezení počítačového systému nebo k učinění počítačového systému neupotřebitelným, nebo ke zničení, poškození nebo změně dat uložených v počítačovém systému nebo na nosiči informací nebo k učinění těchto dat neupotřebitelnými.“

U nejméně závažných útoků s nižší společenskou nebezpečností (v porovnání s jinými závažnými kybernetickými útoky) by tak při potrestání na samotné spodní hranici trestní sazby zůstala zachována možnost podmíněného odložení výkonu trestu dle ustanovení § 81 TZ, ale zároveň by vzhledem k vysoké horní hranici trestní sazby byla trestná již příprava ransomware útoku.

Závěr

V této práci jsem se snažil představit ransomware jako fenomén kyberbezpečnostní, kriminologický a trestněprávní. Ransomware je však primárně fenoménem společenským, který zasahuje již do většiny oblastí lidské činnosti, od průmyslové výroby a služeb, přes zdravotnictví a veřejnou správu, až po běžný rodinný život. Stále četnější ransomware útoky plní stránky světových i domácích médií; zaměstnanci pracující v kancelářích se s pojmem ransomware pravidelně setkávají, v tom lepším případě na povinných školeních a v pravidelných e-mailových zprávách od manažerů kybernetické bezpečnosti; nemocnice, úřady i společnosti se děsí, že právě ony budou terčem příštího kybernetického útoku; řady rodin namísto oblíbeného večerního pořadu zvažují zaplacení výkupného výměnou za odblokování chytré televize.

Téma této práce jsem volil na podzim roku roku 2019. V té době bylo zřejmé, že ransomware útoky jsou na vzestupu, co se týče jejich množství, pokročilosti technologií i financování. Tehdejší hlavní globální ransomware hrozbou byl *Ryuk*, který napadal především velké společnosti a veřejné subjekty včetně nemocnic. V listopadu 2019 jsem však zatím neměl tušení, jak moc důležitým a aktuálním se toto téma stane. Nedlouho po zvolení tématu práce došlo k útoku ransomwaru *Ryuk* na Benešovskou nemocnici, následoval totožný útok proti systémům těžařské společnosti OKD. Ransomware se na určitou dobu stal v českých médiích tématem číslo jedna, představa kompletního vyřazení počítačových systémů nemocnice z provozu a s tím související omezení zdravotní péče, a to všechno v důsledku těžko odvratitelného útoku směřujícího odkudkoliv na světě, je představou, která zneklidní i naprostého kyberbezpečnostního laika.

Příchod globální pandemie v roce 2020 posunul nebezpečnost kybernetických útoků proti nemocnicím na zcela novou úroveň, se zvýšenými riziky na životě a zdraví osob se přitom zvýšila i ochota nemocnic požadované výkupné zaplatit, což vedlo k ještě častějším útokům, ke zvýšení hladiny požadovaného výkupného a k celkové finanční i personální expanzi tohoto zločinného byznysu. V současné době se často říká, že čelíme nikoliv jedné, ale rovnou dvěma globálním pandemiím. Tou druhou je pandemie ransomware.

Jedním ze stanovených cílů práce byl kriminologický rozbor fenoménu ransomware s důrazem na otázku jeho etiologie, dále na kriminologický rozbor osoby pachatele a rovněž na popis viktimologických faktorů a nastínění možností prevence proti ransomware útoku. Z hlediska naplnění tohoto cíle je relevantní především druhá část této práce, ve které jsem dospěl k závěru,

že konflikt v hodnotách hacker culture a většinové společnosti může být jedním z kriminogenních faktorů ovlivňujících vznik kyberkriminálního chování, například v podobě šíření ransomware. Na příčiny vzniku kriminálního chování spočívajícího v šíření ransomware jsem se pokoušel pohlížet optikou kriminologické teorie subkultur a na ni navázané teorie neutralizace Davida Matzy a Greshama Sykese, přičemž jsem uvedl, že lze tyto teorie uplatnit na problematiku ransomware do určité míry. Lépe dle mých závěrů problematiku ransomware vystihuje kriminologická teorie Karuppannana Jaishankara s názvem *space transition theory*, která je zaměřená výhradně na kybernetickou kriminalitu. Ke svým závěrům jsem dospěl otestováním jednotlivých základních postulátů space transition theory v kontextu šíření ransomware, pro ověření správnosti těchto tezí bude však zapotřebí širší výzkum. V dalších kapitolách obsažených v této části jsem představil problém latence kybernetické kriminality, která se týká i ransomware, a popsal jsem nejvýznamější příčiny tohoto jevu. Uvedl jsem přitom jak příčiny latence kybernetické kriminality z obecného hlediska, tak i příčiny latence specifické pro ransomware. Významnou část kriminologické části jsem věnoval popisu oběti a viktimologických faktorů, přičemž jsem dospěl k závěru, že obětí cílených ransomware útoků jsou nejčastěji významné podnikatelské subjekty (především se jedná o subjekty podnikající ve finančním sektoru či ve výrobě), dále nemocnice a systémy veřejné správy. Mezi významné viktimologické faktory můžeme dle mých zjištění mimo jiné zařadit i zaplacení výkupného při předchozím ransomware útoku. U nahodilých obětí je nejvýznamějším viktimologickým faktorem jejich rizikové chování. Rovněž jsem představil možnosti prevence proti šíření ransomware a zdůraznil skutečnost, že prevence je v případě ransomware nejúčinnějším způsobem obrany. V kapitole zaměřující se na aktuální problémy spojené s ransomware jsem se zabýval čím dál častějšími útoky na nemocnice a jiná zdravotnická zařízení, přičemž jsem uvedl, proč jsou nemocnice pro útočníky natolik lákavým cílem. V podkapitole o vztahu pandemie COVID-19 a ransomware jsem uvedl, že mezi těmito jevy existuje vztah přímé úměrnosti, kdy se zvyšující se škodlivostí útoků ransomware roste i ochota obětí platit požadované výkupné. Rovněž jsem se zabýval otázkami vztahu ransomware a hacktivismu, kyberterorismu a kybernetické války. Otevřel jsem také stále aktuálnější téma ransomware zaměřených proti prvkům IoT. V kapitole o prognóze budoucího vývoje ve shodě s odborníky předvídám další rozvoj tohoto fenoménu i v následujících letech s tím, že ransomware útoky budou stále více zacílené na konkrétní subjekty, namísto jejich plošného rozesílání.

Co se týče druhého cíle práce, tedy trestněprávní kvalifikace šíření ransomware, pokusil jsem se oproti jiným pracím obdobného zaměření trestněprávně kvalifikovat šíření ransomware s ohledem na diferenciaci jeho jednotlivých typů. Obvyklým diferenciačním znakem různých typů

ransomware je to, čím je oběti vyhrožováno. Může se jednat o ztrátu dat, zablokování zařízení, zveřejnění citlivých informací či o hrozbu trestním stíháním. Zpravidla tak součástí mého rozboru bylo, zda a za jakých okolností lze danou pohrůžku subsumovat pod zákonný znak pohrůžky jiné těžké újmy ve smyslu trestného činu vydírání. Rovněž byla součástí rozboru úvaha o možné subsumpci funkcionality jednotlivých typů ransomware pod některý ze znaků ustanovení § 230 TZ. Rozbor však nezahrnoval toliko tyto dvě skutkové podstaty, ale celou řadu dalších skutkových podstat trestných činů napříč zvláštní částí trestního zákoníku.

Co se týče stanovených dílčích cílů, jedním z nich bylo kriticky zhodnotit stávající úpravu treněprávní odpovědnosti za šíření ransomware, věnoval jsem se kritickému rozboru současné právní úpravy počítačových trestných činů, kdy jsem vytknul daným ustanovením přílišnou kazuističnost. Následoval konkrétní návrh *de lege ferenda*, včetně konkrétní textace navrhovaného ustanovení, které zohledňovalo mnou tvrzený nedostatek spočívající v beztrestnosti některých forem přípravy šíření ransomware a zvýšenou společenskou nebezpečnost tohoto typu kriminálního chování.

Seznam použitých zdrojů

Seznam použité literatury

BATES, Jim. *Technical analysis: Trojan Horse: AIDS Information Introductory Diskette Version 2.0*. Virus Bulletin. Oxon: Virus Bulletin, 1990(January), ISSN 0956-9979

BRONIEK, David. *Analýza malware.* Ostrava. 2019. Diplomová práce. Vysoká škola báňská – Technická univerzita Ostrava, Fakulta elektrotechniky a informatiky. Vedoucí práce prof. Ing. Ivan Zelínka, Ph.D.

CASTELLS, Manuel. *The Internet Galaxy*. New York: Oxford University Press, 2001. ISBN 0-19-924153-8

DENNING, Dorothy. *Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy*. In: ARQUILLA, John, RONFELDT, David. *Networks and Netwars*. Santa Monica: RAND Corporation, 2001. ISBN 0-8330-3030-2

DIANIŠKA, Gustáv. *Kriminológia*. Plzeň: Aleš Čeněk. 2009. ISBN 978-80-7380-198-4

GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ, Ivana a kol. *Kriminologie. 5. aktualizované vydání*. Praha: Wolters Kluwer ČR, 2019. ISBN 978-80-7598-554-5.

HAYEK, Friedrich August von. *Osudná domýšlivost: omyly socialismu*. Praha: Sociologické nakladatelství, 1995. ISBN 80-858-5005-2.

HOLT, Thomas J., BOSSLER, Adam M. *Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization*. Deviant Behavior. 2008, 30(1), 1-25. ISSN 0163-9625. Dostupné z: doi:10.1080/01639620701876577

JAISHANKAR, Karupannan. *Space transition theory of cyber crimes*. In SCHMALLEGER, Frank, PITTARO, Michael. Crimes of the Internet. New Jersey: Prentice Hall. 2008. ISBN: 978-0132318860

JELÍNEK, Jiří. *Trestní právo hmotné: obecná část, zvláštní část. 6. aktualizované a doplněné vydání*. Praha: Leges, 2017. ISBN 978-80-7502-236-3

JOHANOVSKÝ, Tomáš. *Kriminologické a trestněprávní aspekty fenoménu ransomware*. Praha. 2018. Diplomová práce. Univerzita Karlova, Právnická fakulta. Vedoucí práce doc. JUDr. Tomáš Gřivna, Ph. D.

KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-18-8.

KRUPIČKA, Jiří. *Trestněprávní a kriminologické aspekty internetové kriminality.* Praha, 2012. Disertační práce. Univerzita Karlova, Právnická fakulta. Vedoucí práce prof. JUDr. Jiří Jelínek, CSc.

KUDRLOVÁ, Kateřina. *Avatar jako kriminogenní faktor*. In: SVATOŠ, Roman, KŘÍHA, Josef. (eds.) II. kriminologické dny. České Budějovice: Vysoká škola evropských a regionálních studií, 2014. ISBN 978-80-87472-65-1.

LEVY, Steven. *Hackers: heroes of the computer revolution*. New York: Penguin Books, 2001. ISBN 0-14-100051-1

MATZA, David. *Delinquency and Drift*. London: Routledge. 1990. ISBN: 978-0887388040.

MELAND, Per Hakon, BAYOUMY, Yara Fareed Fahmy, SINDRE, Guttorm. *The Ransomware-as-a-Service economy within the darknet*. Computers & Security. 2020 (February). ISSN 0167-4048. Dostupné z: https://doi.org/10.1016/j.cose.2020.101762

MORRIS, Robert G., *Computer Hacking and the Techniques of Neutralization: An Empirical Assessment*, 2010. [online]. [cit. 2021-6-14]. Dostupné z: doi: 10.4018/978-1-61692-805-6.ch001

MUNKOVÁ, Gabriela. *Sociální deviace. Přehled sociologických teorií*. Plzeň: Aleš Čeněk. 2013. ISBN: 978-80-7380-398-8

POLČÁK. Radim. *Autoritativní regulace kyberprostoru a legitimita trestního práva*. In GŘIVNA, Tomáš, POLČÁK Radim. *Kyberkriminalita a právo*. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4.

PRUCHER, Jeff. *Brave New Words: The Oxford Dictionary of Science Fiction*. Oxford; New York: Oxford University Press, 2007. ISBN 0-19-530567-1.

SMEJKAL, Vladimír. *Kybernetická kriminalita. 2. rozšířené a aktualizované vydání*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7

STRAKA, Václav. *Kybernetická kriminalita z trestněprávního pohledu*. Brno, 2020. Diplomová práce. Masarykova univerzita Právnická fakulta. Vedoucí práce doc. JUDr. Josef Kuchta CSc.

SYKES, Gresham M'Cready, MATZA, David. *Techniques of Neutralization: A Theory of Delinquency*. American Sociological Review. 1957, 22(6). ISSN 00031224. Dostupné z: doi:10.2307/2089195

ŠÁMAL, Pavel a kol. *Trestní zákoník. 2. vydání*. Praha: C. H. Beck, 2012, ISBN 978-80-7400-428-5

VLACH, Jiří, KUDRLOVÁ, Kateřina, PALOUŠOVÁ, Viktorie. *Kyberkriminalita v kriminologické perspektivě*. Praha: Institut pro kriminologii a sociální prevenci. 2020. ISBN: 978-80-7338-189-9

WALL, David S. *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press. 2007. ISBN: 978-0-7456-2736-6

WALL, David. *Cybercrimes: New Wine, No Bottles?* 1999. In: DAVIES, Pamela, FRANCIS, Peter, JUPP, Victor, *Invisible Crimes*. London: Palgrave Macmillan. 1999. ISBN: 978-1-349-27641-7. Dostupné také z: doi: 10.1007/978-1-349-27641-7.

WILLIAMS, Matthew. *Virtually criminal: Crime, deviance and regulation online*. London: Routledge. 2006. ISBN: 978-0-415-36405-8

YAR, Majid. *Cybercrime and society*. London: SAGE Publications, 2006. ISBN 978-1-4129-0753-8

YUNG, Moti, YOUNG, Adam. *Cryptovirology: extortion-based security threats and countermeasures*. IEEE Symposium on Security and Privacy. Oakland: IEEE Comput. Soc. Press, 1996. ISBN 0-8186-7417-2. Dostupné z: doi:10.1109/SECPRI.1996.502676

ZAHRA, Syed Rameem, CHISHTI Mohammad Ahsan. *RansomWare and Internet of Things: A New Security Nightmare*. In: 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence). IEEE, 2019, 2019, s. 551-555. ISBN 978-1-5386-5933-5. Dostupné z: doi:10.1109/CONFLUENCE.2019.8776926

Seznam použitých internetových zdrojů

A Look into the Lazarus Group's Operations. TrendMicro [online]. [cit. 2021-6-30]. Dostupné z: https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/a-look-into-the-lazarus-groups-operations

Adversary: Cozy Bear. Crowdstrike [online]. [cit. 2021-6-30]. Dostupné z: https://adversary.crowdstrike.com/en-US/adversary/cozy-bear/

Andariel evolves to target South Korea with ransomware. SECURELIST [online]. [cit. 2021-6-30]. Dostupné z: https://securelist.com/andariel-evolves-to-target-south-korea-with-ransomware/102811/

APT1. MITRE ATT&CK [online]. [cit. 2021-6-30]. Dostupné z: https://attack.mitre.org/groups/G0006/

ARSENE, Liviu. *5 Times More Coronavirus-themed Malware Reports during March*. Bitdefender [online]. [cit. 2021-6-23]. Dostupné z: https://labs.bitdefender.com/2020/03/5-times-more-coronavirus-themed-malware-reports-during-march/

BARLOW, John Perry. *A Declaration of the Independence of Cyberspace* [online]. [cit. 2021-5-30]. Dostupné z: https://www.eff.org/cyberspace-independence

BUCHTA, Martin. *Jak odstranit policejní vir?* ESET [online]. [cit. 2021-5-25]. Dostupné z: https://servis.eset.cz/knowledgebase/article/View/257/46/jak-odstranit-policejni-vir#.YK4FxagzaUk

BURDOVA, Carly. What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant? Avast [online]. [cit. 2021-9-2]. Dostupné z: https://www.avast.com/c-eternalblue.

Co je to adware? Avast [online]. [cit. 2021-5-30]. Dostupné z: https://www.avast.com/cs-cz/c-adware

Co je Tor? Alza.cz [online]. [cit. 2021-5-21]. Dostupné z: https://www.alza.cz/co-je-tor

COVID-19 Ransomware. EUROPOL [online]. [cit. 2021-6-23]. Dostupné z: https://www.europol.europa.eu/covid-19/covid-19-ransomware

CSIRT.CZ. *Historie a vývoj ransomwaru: všechno to začalo s AIDS*. Lupa.cz [online]. [cit. 2021-5-15]. Dostupné z: https://www.lupa.cz/clanky/historie-a-vyvoj-ransomwaru-vsechno-to-zacalo-s-aids/

Cyber-attack: Europol says it was unprecedented in scale. BBC [online]. [cit. 2021-5-18]. Dostupné z: https://www.bbc.com/news/world-europe-39907965

DICKSON, Ben. *The IoT ransomware threat is more serious than you think*. IoT Security Foundation [online]. [cit. 2021-6-25]. Dostupné z: https://www.iotsecurityfoundation.org/the-iot-ransomware-threat-is-more-serious-than-you-think/¨

Efekt červené královny. Wikipedia [online]. [cit. 2021-7-1]. Dostupné z: https://cs.wikipedia.org/wiki/Efekt_%C4%8Derven%C3%A9_kr%C3%A1lovny

Equation: The Death Star of Malware Galaxy. SecureList [online]. [cit. 2021-6-30]. Dostupné z: https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/

Exploit. Wikipedia [online]. [cit. 2021-5-30]. Dostupné z: https://cs.wikipedia.org/wiki/Exploit

Fox Kitten – Widespread Iranian Espionage-Offensive Campaign. ClearSky [online]. [cit. 2021-6-30]. Dostupné z: https://www.clearskysec.com/fox-kitten/

GLENNY, Misha. *Cybercrime is becoming the mafia's newest racket*. Roland Berger [online]. [cit. 2021-6-18]. Dostupné z: https://www.rolandberger.com/en/Insights/Publications/Cybercrime-is-becoming-the-mafia%E2%80%99s-newest-racket.html

Global ransomware and cyberattacks on healthcare spike during pandemic. Bitdefender [online]. [cit. 2021-6-23]. Dostupné z: https://labs.bitdefender.com/2020/05/global-ransomware-and-cyberattacks-on-healthcare-spike-during-pandemic/

GOODIN, Dan. *Group claims to hack NSA-tied hackers, posts exploits as proof*. ArsTechnica [online]. [cit. 2021-6-30]. Dostupné z: https://arstechnica.com/information-technology/2016/08/group-claims-to-hack-nsa-tied-hackers-posts-exploits-as-proof/

GREENBERG, Andy. *Hackers Remotely Kill a Jeep on the Highway – With Me in It*. Wired [online]. [cit. 2021-6-25]. Dostupné z: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

GRUSTNIY, Leonid. *Smart cars: Comfort costs*. Kaspersky [online]. [cit. 2021-6-25]. Dostupné z: https://www.kaspersky.com/blog/dont-hack-your-car/22090/

Historie ransomware hrozeb: jak to bylo, je a bude. VpnMentor [online]. [cit. 2021-5-18]. Dostupné z: https://cs.vpnmentor.com/blog/historie-ransomware-hrozeb-minulost-soucasnost-budoucnost/

HORÁK, Jan. *Na nemocnici v Brně zaútočil vyděračský virus, špitál povolal krizového IT manažera*. Aktuálně [online]. [cit. 2021-6-23]. Dostupné z: https://zpravy.aktualne.cz/domaci/na-nemocnici-v-brne-zautocil-vyderacsky-virus-spital-povolal/r~ff91a02c6aa011eab1110cc47ab5f122/

Hospitals Targeted in Rising Wave of Ryuk Ransomware Attacks. Check Point [online]. [cit. 2021-5-30]. Dostupné z: https://blog.checkpoint.com/2020/10/29/hospitals-targeted-in-rising-wave-of-ryuk-ransomware-attacks/

IBM SECURITY. *IBM X-Force Threat Intelligence Index. 2021.* [online]. [cit. 2021-6-18]. Dostupné z: https://www.ibm.com/security/data-breach/threat-intelligence

JAISHANKAR, Karuppannan. *Space Transition Theory of Cyber Crimes*. 2008. [online]. [cit. 2021-6-15]. Dostupné z: https://www.researchgate.net/publication/321716315_Space_Transition_Theory_of_Cyber_Crimes

JOHNSON, A. L. *WannaCry: Ransomware attacks show strong links to Lazarus group*. Broadcom [online]. [cit. 2021-5-21]. Dostupné z: https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=b2b00f1b-e553-47df-920d-f79281a80269&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

'Jugular' of the U.S. fuel pipeline system shuts down after cyberattack. Politico [online]. [cit. 2021-6-23]. Dostupné z: https://www.politico.com/news/2021/05/08/colonial-pipeline-cyber-attack-485984

Kaspersky research finds 174 municipal institutions targeted with ransomware in 2019. Kaspersky [online]. [cit. 2021-6-23]. Dostupné z: https://usa.kaspersky.com/about/press-

releases/2019_kaspersky-research-finds-174-municipal-institutions-targeted-with-ransomware-in-2019

KRUPKA, Jaroslav. *Globální kyberútok vyřadil počítače s Windows XP, uvedla britská ministryně.* Deník.cz [online]. [cit. 2021-6-30]. Dostupné z: https://www.denik.cz/ze_sveta/kyberutok-vyradil-pocitace-s-windows-xp-uvedla-britska-ministryne.html

Kyberpunk. Wikipedia [online]. [cit. 2021-4-19]. Dostupné z: https://cs.wikipedia.org/wiki/Kyberpunk

Lazarus Group. MITRE ATT&CK [online]. [cit. 2021-6-30]. Dostupné z: https://attack.mitre.org/groups/G0032/

MACEK, Jakub. *Kyberprostor*. Revue pro média [online]. [cit. 2021-05-07]. Dostupné z: http://rpm.fss.muni.cz/Revue/Heslar/ kyberprostor.htm

MACFARLANE, Alec. *Why the massive cyberattack won't make the hackers rich*. CNN Business [online]. [cit. 2021-5-21]. Dostupné z: https://money.cnn.com/2017/05/17/technology/wannacry-ransomware-bitcoin-cyberattack/index.html

MELTZER, Tom, PHILLIPS, Sarah. *From the first email to the first YouTube video: a definitive internet history*. The Guardian [online]. [cit. 2021-5-30]. Dostupné z: https://www.theguardian.com/technology/2009/oct/23/internet-history

MUNCASTER, Phil. *Two More Lazarus Group Members Indicted for North Korean Attacks*. Infosecurity [online]. [cit. 2021-6-30]. Dostupné z: https://www.infosecurity-magazine.com/news/lazarus-group-indicted-north/?__cf_chl_jschl_tk__=pmd_69d42cda2938341282cef6e5cbce05bb5e9cb36e-1626893792-0-gqNtZGzNAfijcnBszQqO

Národní knihovna se stala terčem útoku hackerů. Vedení odstavilo systémy a podalo trestní oznámení. iRozhlas [online]. [cit. 2021-9-2]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/narodni-knihovna-hackersky-utok_2105181615_pj

Nejvyšší žalobce Zeman: Zločinci se přesouvají do kyberprostoru. Novinky.cz [online]. [cit. 2021-6-1]. Dostupné z: https://www.novinky.cz/domaci/clanek/nejvyssi-zalobce-zeman-zlocinci-se-presouvaji-do-kyberprostoru-18402

NG, Alfred. *US: Russia's NotPetya the most destructive cyberattack ever.* CNet [online]. [cit. 2021-9-2]. Dostupné z: https://www.cnet.com/tech/services-and-software/uk-said-russia-is-behind-destructive-2017-cyberattack-in-ukraine/

No More Ransom! [online]. [cit. 2021-6-22]. Dostupné z: https://www.nomoreransom.org/cs/about-the-project.html

Olomoucký magistrát čelí několik týdnů hackerským útokům. Odmítá zaplatit výkupné. iRozhlas [online]. [cit. 2021-9-2]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/olomouc-magistrat-hackersky-utok-hackeri-ransomware-avaddon_2105221133_ako

Phishingové útoky už dávno nejsou jen hloupé. Computerworld [online]. [cit. 2021-5-15]. Dostupné z: https://computerworld.cz/securityworld/phishingove-utoky-uz-davno-nejsou-jen-hloupe-50888

Pokročilá trvalá hrozba. Wikipedie [online]. [cit. 2021-6-30]. Dostupné z: https://cs.wikipedia.org/wiki/Pokro%C4%8Dil%C3%A1_trval%C3%A1_hrozba

Policie ČR vás sleduje! Viry.cz [online]. [cit. 2021-5-18]. Dostupné z: https://viry.cz/policie-cr-vas-sleduje/

Ransomware - What is it & how to remove it? Malwarebytes [online]. [cit. 2021-5-14]. Dostupné z: https://www.malwarebytes.com/ransomware/

Ransomware as a Service (RaaS) explained. Crowdstrike [online]. [cit. 2021-5-25]. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/

Ransomware: A billion-dollar problem. Blog.avast [online]. [cit. 2021-5-14]. Dostupné z: https://blog.avast.com/ransomware-a-billion-dollar-problem

Ransomware: The True Cost To Business. 2021. Cybereason [online]. [cit. 2021-6-20]. Dostupné z: https://www.cybereason.com/ebook-ransomware-the-true-cost-to-business

Ransomware-as-a-service: The pandemic within a pandemic. Intel471 [online]. [cit. 2021-5-30]. Dostupné z: https://intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/

Russian criminal group suspected in Colonial pipeline ransomware attack. NBC News [online]. [cit. 2021-6-23]. Dostupné z: https://www.nbcnews.com/politics/national-security/russian-criminal-group-may-be-responsible-colonial-pipeline-ransomware-attack-n1266793

SANMILLAN, I. *Ramsay: A cyber-espionage toolkit tailored for air-gapped networks*. ESET [online]. [cit. 2021-6-20]. Dostupné z: https://www.welivesecurity.com/2020/05/13/ramsay-cyberespionage-toolkit-airgapped-networks/

SCAM419 [online]. [cit. 2021-5-14]. Dostupné z: https://www.hoax.cz/scam419/

SOARE, Bianca. *Operation Tovar: What It Was and How A Key Botnet Was Eliminated*. Heimdal security [online]. [cit. 2021-5-21]. Dostupné z: https://heimdalsecurity.com/blog/operation-tovar/

Společenská smlouva. Wikipedia [online]. [cit. 2021-5-30]. Dostupné z: https://cs.wikipedia.org/wiki/ Spole%C4%8Densk%C3%A1_smlouva

STROM, David. *The rise of ransomware as a service*. Avast Blog [online]. [cit. 2021-5-25]. Dostupné z: https://blog.avast.com/ransomware-as-a-service-avast

STUBBS, Jack. *Exclusive: Suspected North Korean hackers targeted COVID vaccine maker AstraZeneca - sources.* Reuters [online]. [cit. 2021-6-30]. Dostupné z: https://www.reuters.com/article/us-healthcare-coronavirus-astrazeneca-no-idUSKBN2871A2

TALAMANTES, Jeremiah. *USB Drop Attacks: The Danger Of "Lost And Found" Thumb Drives*. RedTeam Security [online]. [cit. 2021-6-20]. Dostupné z: https://www.redteamsecure.com/blog/usb-drop-attacks-the-danger-of-lost-and-found-thumb-drives

The hospital held hostage by hackers. CNBC [online]. [cit. 2021-6-22]. Dostupné z: https://www.cnbc.com/2016/02/16/the-hospital-held-hostage-by-hackers.html

Truth in malvertising: How to beat bad ads. Malwarebytes [online]. [cit. 2021-5-15]. Dostupné z: https://blog.malwarebytes.com/101/2016/06/truth-in-malvertising-how-to-beat-bad-ads/

TUNG, Liam. *Europol warns of IoT murder and ransomware for smart cars*. ZDnet [online]. [cit. 2021-6-25]. Dostupné z: https://www.zdnet.com/article/europol-warns-of-iot-murder-and-ransomware-for-smart-cars/

Úmrtí kvůli hackerskému útoku? Byla to jen otázka času, míní bezpečnostní expert. Novinky.cz [online]. [cit. 2021-6-22]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/umrti-kvuli-hackerskemu-utoku-byla-to-jen-otazka-casu-mini-bezpecnostni-expert-40337662

What is maze ransomware? Definition and explanation. Kaspersky [online]. [cit. 2021-5-21]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/what-is-maze-ransomware

Who is FANCY BEAR (APT28)? Crowdstrike [online]. [cit. 2021-6-30]. Dostupné z: https://www.crowdstrike.com/blog/who-is-fancy-bear/

Yahoo users hit by 'malvertising' campaign. The Guardian [online]. [cit. 2021-5-15]. Dostupné z: https://www.theguardian.com/technology/2015/aug/05/yahoo-users-malvertising-campaign-malware

Za útokem na benešovskou nemocnici byl ruský vir Ryuk. ČT24 [online]. [cit. 2021-5-30]. Dostupné z: https://ct24.ceskatelevize.cz/regiony/stredocesky-kraj/3029729-za-utokem-na-benesovskou-nemocnici-byl-rusky-vir-ryuk

ZAHARIA, Andra. *Security Alert: New and Cheap Stampado Ransomware for Sale on the Dark Web*. Heimdal security [online]. [cit. 2021-5-25]. Dostupné z: https://heimdalsecurity.com/blog/security-alert-stampado-ransomware-on-sale/

ZOULOVÁ, Lenka. *Úmrtí kvůli hackerskému útoku? Byla to jen otázka času, míní bezpečnostní expert*. Novinky.cz [online]. [cit. 2021-5-30]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/umrti-kvuli-hackerskemu-utoku-byla-to-jen-otazka-casu-mini-bezpecnostni-expert-40337662

Seznam použitých právních předpisů

Dodatkový protokol k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů ze dne 28. 1. 2003 (vyhlášen pod č. 9/2015 Sb. m. s.)

ETS No.185 – Úmluva Rady Evropy č. 185 ze dne 23. 11. 2001 o počítačové kriminalitě (vyhlášená pod č. 104/2013 Sb. m. s.)

Zákon č. 141/1961 Sb. o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů

Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů

Zákon č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů (zákon o soudnictví ve věcech mládeže), ve znění pozdějších předpisů

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

Seznam použité judikatury

Rozsudek Nejvyššího soudu ze dne 8. 4. 1981, sp. zn. 6 Tz 12/81

Usnesení Nejvyššího soudu ze dne 23. 1. 2007, sp. zn. 11 Tdo 1545/2006

Usnesení Nejvyššího soudu ze dne 15. 6. 2011, sp. zn. 8 Tdo 612/2011

Usnesení Nejvyššího soudu ze dne 24. 2. 2015, sp. zn. 6 Tdo 1480/2014

Usnesení Nejvyššího soudu ze dne 14.06.2016, sp. zn. 7 Tdo 650/2016

Seznam použitých obrázků

Obrázek č. 1 – *AIDS Trojan* [online]. [cit. 2021-5-1]. Dostupné z: https://en.wikipedia.org/wiki/AIDS_(Trojan_horse)#/media/File:AIDS_DOS_Trojan.png

Obrázek č. 2 – *WannaCry ransom note* [online]. [cit. 2021-5-1]. Dostupné z: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#/media/File:Wana_Decrypt0r_screenshot.png

Obrázek č. 3 – *Jedna z variant policejního viru* [online]. [cit. 2021-5-1]. Dostupné z: https://www.policie.cz/clanek/objevuje-se-vam-na-monitoru-podezrele-hlaseni.aspx

Obrázek č. 4 – *Model space transition theory* [online]. [cit. 2021-5-1]. Dostupné z: https://www.researchgate.net/publication/321716315_Space_Transition_Theory_of_Cyber_Crimes

Obrázek č. 5 – *Počet ransomware útoků na nemocniční zařízení (oranžová) a počet napadených lékařských záznamů pacientů (modrá) ve Spojených státech mezi lety 2016 a 2020* [online]. [cit. 2021-5-1]. Dostupné z: https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/

Seznam ostatních zdrojů

Bezpečnostní informační služba. *Výroční zpráva bezpečnostní informační služby pro rok 2019*. 2020. [online]. [cit. 2021-6-15]. Dostupné z: https://www.bis.cz/vyrocni-zpravy/vyrocni-zprava-bezpecnostni-informacni-sluzby-za-rok-2019-c665e2a7.html

JAISHANKAR, Karupannan. *What can human behavior online suggest about cyber crime.* YouTube [videopřednáška online]. [cit. 2021-4-19]. Dostupné z: https://www.youtube.com/watch?v=Oiv6VK-FjAc

Národní centrála proti organizovanému zločinu služby kriminální policie a vyšetřování. *Výroční zpráva 2020*. [online]. [cit. 2021-6-30]. Dostupné z: https://www.policie.cz/clanek/web-informacni-servis-zpravodajstvi-vyrocni-zprava-ncoz-2020.aspx?fbclid=IwAR3HaMBspl-4Nf2vIZfQWHkzzEoJ_OWK7g2fECbBoGal7deURIZJ9XKaFzQ

Národní úřad pro kybernetickou a informační bezpečnost ČR. *Analýza hrozby ransomware*. [cit. 2021-5-30] Dostupné z: https://nukib.cz/download/publikace/analyzy/Analyza_hrozby_ransomware.pdf

Národní úřad pro kybernetickou a informační bezpečnost ČR. *Upozornění na probíhající kampaň ransomwaru Avaddon* [online]. [cit. 2021-5-30]. Dostupné z: https://www.nukib.cz/cs/infoservis/hrozby/1717-upozorneni-na-probihajici-kampan-ransomwaru-avaddon/

Národní úřad pro kybernetickou a informační bezpečnost ČR. *Vyděračské útoky ransomwarem jsou cílenější: míří na velké firmy, státní a veřejné instituce.* 2020. [online]. [cit. 2021-6-21].

Dostupné z: https://www.nukib.cz/download/publikace/analyzy/Analyza_hrozby_ransomware.pdf

Národní úřad pro kybernetickou a informační bezpečnost ČR. *Zpráva o stavu kybernetické bezpečnosti ČR - 2019* [online]. [cit. 2021-5-1]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/NUKIB_ ZSKB_2019.pdf

Národní úřad pro kybernetickou a informační bezpečnost. *Upozornění na zvýšené riziko kybernetických útoků proti ČR*. [online]. [cit. 2021-6-23]. Dostupné z: https://www.nukib.cz/cs/infoservis/aktuality/1703-hrozi-zvysene-riziko-kybernetickych-utoku-vuci-ceske-republice/

Statistické přehledy kriminality za rok 2019. Policie ČR [online]. [cit. 2021-6-30]. Dostupné z: https://www.policie.cz/clanek/statisticke-prehledy-kriminality-za-rok-2019.aspx

Statistické přehledy kriminality za rok 2020. Policie ČR [online]. [cit. 2021-6-30]. Dostupné z: https://www.policie.cz/clanek/statisticke-prehledy-kriminality-za-rok-2020.aspx

Středočeští kriminalisté ukončili vyšetřování Ransomware útoku na benešovskou nemocnici. Policie ČR [online]. [cit. 2021-6-22]. Dostupné z: https://www.policie.cz/clanek/stredocesti-kriminaliste-ukoncili-vysetrovani-ransomware-utoku-na-benesovskou-nemocnici.aspx

Vyjádření k okolnostem vyhoštění 18 zaměstnanců ruské ambasády. Vláda ČR [online]. [cit. 2021-6-23]. Dostupné z: https://www.vlada.cz/cz/media-centrum/aktualne/vyjadreni-k-okolnostem-vyhosteni-18-zamestnancu-ruske-ambasady-187806/

Trestněprávní a kriminologické aspekty šíření ransomware

Abstrakt

Předmětem této diplomové práce je šíření ransomware, které je aktuálně jednou z nejzásadnějších globálních kybernetických hrozeb. Ransomware je škodlivý kód, který při své aktivaci v počítačovém systému zpravidla zablokuje přístup k tomuto systému či zašifruje data v něm obsažená, na základě čehož poté uživatele vydírá. Tato práce se zabývá kriminologickými a trestněprávními aspekty tohoto fenoménu.

Ve své kriminologické části se tato práce zabývá otázkou etiologie šíření ransomware a kriminogenními faktory, přičemž mimo jiné zkoumá aplikovatelnost kyberkriminologické teorie *space transition theory* na daný fenomén. Dále se zabývá viktimologickým aspektem věci, přičemž vyjmenovává nejzásadnější faktory ovlivňující viktimizaci, a to jak v případě plošných nezacílených ransomware útoků, tak v případě útoků konkrétně zacílených. Rovněž zkoumá otázku vysoké latence tohoto fenoménu a kyberkriminality obecně a možnosti prevence, kterou hodnotí jako nejlepší způsob obrany proti ransomware útoku. Zvlášť se zabývá otázkou ransomware útoků na nemocnice a kritickou infrastrukturu, otevírá rovněž téma nárustu počtu útoků v důsledku pandemie COVID-19. Obsažena je i problematika politicky motivovaných kybernetických útoků. V závěru kriminologické části je uvedena prognóza budoucího vývoje, ne příliš optimistická.

Ve své trestněprávní části se tato práce zabývá především právní kvalifikací šíření ransomware z pohledu českého trestního práva hmotného. Ojedinělá je tato práce v tom aspektu, že se zabývá trestněprávní kvalifikací šíření ransomware s ohledem na různé druhy ransomware, jako je šifrovací ransomware, locker ransomware či policejní virus. Následuje kritické zhodnocení současné právní úpravy trestní odpovědnosti za tento typ kriminálního chování a závěrem je představen konkrétní návrh *de lege ferenda*.

Klíčová slova: ransomware, kybernetická kriminalita, kyberprostor

Criminological and criminal law aspects of the ransomware spread

Abstract

The subject of this diploma thesis is the ransomware spread, which is currently one of the most prominent global cybernetic threats. Ransomware is malicious code that, when activated on a computer system, usually blocks access to that system or encrypts the data contained in it, which is then used to blackmail the user. This thesis deals with criminological and criminal aspects of this phenomenon.

In its criminological part, this thesis deals with the issue of the etiology of the ransomware spread and its criminogenic factors, while examining, among other things, the applicability of cybercriminological theory named *space transition theory* to a given phenomenon. It also deals with the victimological aspect of the matter, listing the most fundamental factors influencing victimization, both in the case of widespread non-targeted ransomware attacks and in the case of specifically targeted attacks. It also examines the issue of the high latency of this phenomenon and cybercrime in general and the possibility of prevention, which it considers to be the best way to defend against a ransomware attack. In particular, it deals with the issue of ransomware attacks on hospitals and critical infrastructure, and also raises the issue of the increase in the number of attacks due to the COVID-19 pandemic. The issue of politically motivated cyber attacks is also included. At the end of the criminological part, the prognosis of future development is given, not very optimistic.

In its criminal law part, this work deals mainly with the legal qualification of the spread of ransomware from the perspective of Czech substantive criminal law. This work is unique in that manner, that it deals with the criminal qualification of the ransomware spread with respect to various types of ransomware, such as crypto ransomware, locker ransomware or police virus. Critical evaluation of the current legislation of criminal liability for this type of criminal behavior follows, and in conclusion, a specific proposal *de lege ferenda* is presented.

Key words: ransomware, cybercrime, cyberspace