VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

VÝVOJ A ASPEKTY KYBERNETICKÉ KRIMINALITY

Autor práce: Jan Vamberský

Studijní obor: Bezpečnostně právní činnost ve veřejné správě

Forma studia: Kombinovaná

Vedoucí práce: RNDr. Růžena Ferebauerová

Katedra: Katedra právních oborů a bezpečnostních studií

2019

Prohlašuji, že jsem bakalářskou práci vypracoval(a) samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce – v elektronické podobě ve veřejně přístupné části infodisku VŠERS a v tištěné podobě knihovnou VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucího a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucímu bakalářské práce, paní RNDr. Růženě Ferebauerové, za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

VAMBERSKÝ, J. Vývoj a aspekty kybernetické kriminality: *bakalářská práce.* České Budějovice : Vysoká škola evropských a regionálních studií, 2019. 61 s. Vedoucí bakalářské práce : RNDr. Růžena Ferebauerová

Klíčová slova: kybernetická kriminalita, informační a komunikační technologie, kyberprostor, Internet, kybernetické útoky, informační bezpečnost, prevence

Předmětem bakalářské práce je v dostatečné míře shrnout problematiku kybernetické kriminality, trestné činnosti spojené s vývojem informačních a komunikačních technologií a rozmachem Internetu. Po vymezení základních pojmů a definic jsou zmapovány historické etapy tohoto protiprávního jednání, specifikovány jednotlivé formy kybernetických útoků, kdy jsou informační technologie jednak jejich terčem, jednak nástrojem k jejich páchání. Následuje přehled legislativní úpravy v mezinárodním a českém prostředí. Nastíněny jsou i metody vyšetřování. Cílem této práce je podat ucelený pohled na tento vysoce nebezpečný fenomén s doporučením základních pravidel možné prevence, nikoliv danou problematiku řešit či hodnotit.

ABSTRACT

VAMBERSKÝ, J. The Development and Aspects of Cyber Crime: Bachelor Thesis. České Budějovice: The College of European and Regional Studies, 2019. 61 p. Supervisor: RNDr. Růžena Ferebauerová

Key words: Cybercrime, Information and Communication Technologies, Cyberspace, Internet, Cyber Attacks, Information Security, Prevention

The aim of this bachelor thesis is to provide an overview of cybercrime and the criminal activities associated with the development of information and communication technologies and the rapid expansion of the Internet. After the basic concepts and terms have been defined, the historical stages of this illegal activity are charted and the individual forms of cyber attacks specified in terms of when information technology is the target, and when it is the weapon used in order to carry out such attacks. There follows an overview of legislation on both an international and Czech level and an outline of investigative methods. This thesis aims to offer a compact survey of this highly dangerous phenomenon and a recommendation of the basic rules of possible prevention, but not to resolve or evaluate the problematic.

Obsah

Úvod

V dnešní době je počítač základním vybavením téměř každé domácnosti a nepostradatelným pomocníkem subjektů ať už v komerční nebo státní sféře v různých oborech a odvětvích, včetně institucí na strategické úrovni. Stejně tak si nedovedeme představit život bez připojení k Internetu, který je nejen zdrojem informaci, ale především nástrojem komunikace napříč zeměkoulí. Provoz výpočetní techniky, komunikačních prostředků a informačních systémů usnadňuje práci a šetří čas, umožňuje spojení se světem, avšak bez patřičné obezřetnosti a řádného zabezpečení se mohou osobní údaje, důvěrné informace a materiály nebo finanční prostředky lehce ocitnout v nesprávných rukou. Zneužití těchto dat a informací může zásadně ovlivnit nejen život jedince, existenci firmy, ale také ohrozit vývoj či zájmy naší společnosti a to v celosvětovém měřítku. Problematika trestné činnosti páchané touto formou je proto více než aktuální. Dostupná čísla jasně ukazují každoroční nárůst tohoto nebezpečného protiprávního jednání, který je přímo úměrný rychlému vývoji a růstu informačních a komunikačních technologií. Odhalování zločinů páchaných pomocí počítače, proti jinému počítači nebo počítačové síti je velmi náročné. Sofistikovanost těchto útoků klade vysoké nároky na neustálé prohlubování znalostí specialistů z řad policie, kteří se zabývají získáním důkazního materiálu a prokázáním identifikace pachatele. I aplikovaná metodika vyšetřování se specifickými postupy je zcela odlišná u kyberkriminality ve srovnání s ostatními druhy trestné činnosti. Spolupráce orgánů činných v trestním řízení probíhá mnohdy na mezinárodní úrovni, neboť zločiny v kyberprostoru neomezují státní hranice.

Česká republika v roce 2005 podepsala a o několik let později ratifikovala první mezinárodní Úmluvu o počítačové kriminalitě, která je kromě evropských států závazná i pro USA a Japonsko. Definuje sjednocení skutkových podstat této trestné činnosti s jasným cílem zjednodušení procesu spolupráce jednotlivých členských států s vytýčením mezinárodního postihu. V České republice současný trestní zákoník (zákon č. 40/2009 Sb.), termín kybernetická kriminalita jako takový nespecifikuje, pro potírání těchto trestných činů ale obsahuje dostatečný výčet dotčených skutkových podstat.

Kromě potírání kybernetické kriminality příslušnými orgány je však třeba řešit především zabezpečení. Zásadním legislativním počinem, jehož smyslem je právě ochrana funkčnosti kybernetického prostoru, je zákon o kybernetické bezpečnosti. Tento zákon nabyl účinnosti počátkem roku 2015 a upravuje práva a povinnosti

dotčených subjektů v oblasti zajištění bezpečnosti informačních a komunikačních systémů, jakožto i pravomoc a působnost orgánů veřejné moci.

Základem preventivních opatření ze strany běžných uživatelů by měla být ochrana počítačů a sítí k tomuto určenými dostupnými technickými prostředky, ale neméně podstatná je gramotnost v této oblasti. Důležitá je informovanost o pravidlech návyků a chování při používání informačních a komunikačních technologií zejména rizikových skupin, nejen jejich uživatelské dovednosti.

1 Cíl a metodika bakalářské práce

Cílem bakalářské práce Vývoj a aspekty kybernetické kriminality je podat ucelený pohled na problematiku trestné činnosti v kyberprostoru a s tím spojené kybernetické bezpečnosti.

Pro zpracování tématu byla použita metoda sběru informací studiem odborné literatury, zákonů a dalších dostupných relevantních pramenů. Získaný materiál je pak rozdělen do dvou částí, teoretické a praktické, kdy každá část obsahuje několik na sebe navazujících kapitol.

V první části, jsou nejprve vymezeny základní pojmy a definice. Po stručné historii následující kapitola specifikuje pachatele, jejich metody a samotné formy jednotlivých projevů protiprávních jednání. Další kapitola se věnuje problematice vyšetřování této trestné činnosti. Závěr této části tvoří přehled vývoje mezinárodních a vnitrostátních legislativních opatření k potírání kybernetické kriminality a rovněž z oblasti kybernetické bezpečnosti.

Ve druhé části, jsou pak uvedeny příklady frekventovaných trestních činů na našem území s předpokladem dalšího vývoje. Závěr tvoří analýza v oblasti preventivních opatření, která zahrnuje možnosti zabezpečení, ale zejména poukazuje na nutnost osvěty, kdy gramotnost uživatelů informačních a komunikačních technologií by měla být řazena k základnímu všeobecnému vzdělání.

2 Kybernetická kriminalita

S rozmachem a raketovým vývojem informačních a komunikačních technologií, se kterými se setkáváme téměř ve všech odvětvích lidské činnosti a stávají se tak součástí našeho profesního a běžného života, zákonitě roste i jejich zneužívání. Moderní technologie umožňují zpracování dat a informací formou digitalizace. Z hlediska časového, prostorového a přístupového je implementace těchto velmi často citlivých údajů do informačních systémů velkým přínosem, na druhé straně však jejich bezpečnost může být ohrožena.

Pole působnosti kybernetických útočníků je značně široké a nesoustředí se „jen“ na získání kódů platebních karet a přístupových hesel, ale zejména na manipulaci s citlivými daty. Zcizená data mohou být využita k další podvodné činnosti, nebo zpeněžena. Ohroženi nejsou pouze jedinci, stále odolnější, sofistikované viry pronikají do systémů firem a významných organizací jak z podnikatelské sféry, tak státního sektoru, ohroženy jsou kritické infrastruktury. Cílem útoků organizovaných a vysoce specializovaných skupin mnohdy řízených vládou jiného státu je kybernetická špionáž mířící na ekonomickou, technologickou, vojenskou nebo politickou sféru. Kybernetické útoky tak mohou paralyzovat nejen finanční trhy, řízení letecké dopravy, elektrorozvodné sítě, zdravotnictví, stejně tak jako počítačové sítě obrany státu nebo vlády.

Odborná veřejnost se shoduje na každoročně rostoucím trendu tohoto vysoce společensky škodlivého jednání, což je zjevně způsobeno přesunem trestné činnosti klasifikované jako tradiční do kyberprostoru. Tento fakt v posledních letech také nepochybně ovlivňuje rostoucí ekonomika a s ní spojená vyšší životní úroveň. Kybernetická kriminalita je označována za nejvýnosnější byznys, předčí tak i obchod s drogami, přičemž riziko možnosti dopadení je poměrně nízké. Stanovit výši způsobených škod vzhledem ke globálnosti tohoto jevu je však takřka nemožné, nicméně odhadovaná čísla se pohybují v řádech stovek miliard dolarů ročně. Je předpokládáno, že největší ztráty způsobují krádeže duševního vlastnictví a know-how v oblasti technologií. Obecně se však předpokládá, že nahlášených kybernetických incidentů je pouze zlomek, kdy důvodem je obava ze ztráty dobré pověsti a důvěry svých klientů, zejména jedná-li se o bankovní domy.

Neodmyslitelnou součástí digitálního světa jsou sociální sítě, jejichž prostřednictvím je možná komunikace s kýmkoliv. Stávají se tak fenoménem

současnosti, což samozřejmě přináší i své stinné stránky. Vyvolávají nejen závislost, uživatel může být ohrožen kyberšikanou, ale především sdílené informace a digitální identita uživatele mohou být zneužity třetí osobou.

Technologickým světem však hýbe ještě další věc. Internet věcí (*Internet of Things*), zařízení, vybavených síťovým čipem a softwarem, jejichž vzájemnou komunikaci lze řídit přes chytrý telefon nebo tablet, ať jsme kdekoliv. Pojmem „inteligentní" je označována domácí elektronika, přístroje na sběr zdravotních dat nositele, automobily nebo dokonce celé domy. Nebezpečí však číhá v chabém zabezpečení, kdy útočníci snadno mohou sbírat všechna důvěrná data, nebo způsobit nedozírnou kalamitu jejich přeprogramováním.

Historicky se pro odstartování trestné činnosti v kyberprostoru považují devadesátá léta minulého století, kdy se osobní počítače staly relativně dostupné i pro domácnosti. Dalším významným milníkem je však rozšíření Internetu, celosvětového systému počítačových sítí, umožňující vzdálený přístup k počítači. V tomto období se ustálilo označení *počítačová kriminalita*, později *informační kriminalita*, pro trestné činy páchané proti počítačům nebo pomocí počítače. Technickým pokrokem k uživatelským počítačům přibyly notebooky, netbooky, Ipady a chytré telefony začaly pomalu vytěsňovat pevné linky. I tato masově rozšířená přenosná bezdrátová zařízení obsahující miniaturní mikroprocesory plní funkce osobních počítačů a proto jsou rovněž velmi zajímavým terčem útočníků. V těchto souvislostech termín počítačová resp. informační kriminalita byl modifikován na **kybernetická kriminalita**.

Nejobecněji je možné kybernetickou kriminalitu definovat jako jednání namířená proti počítači, případně síti, nebo jako jednání, při němž je počítač použit jako nástroj pro spáchání trestného činu. Neopomenutelnou skutečností pro to, aby bylo možné uplatnit definici kyberkriminality je to, že počítačová síť (zejména Internet) je pak prostředím, v němž se tato činnost odehrává.[1]

Na tomto místě je třeba osvětlit co je vlastně **kyberprostor**, veřejností vnímán jako Internet. Vstup do tohoto prostředí můžeme sami ovlivnit a to pouhým zapnutím či vypnutím počítače, resp. modemu, nebo chytrého telefonu. Kyberprostorem (z anglického *Cyberspace)* nazýváme virtuální prostředí, jakýsi nehmotný prostor, který vznikl vzájemným propojením počítačových, informačních a komunikačních systémů a

[1] KOLOUCH, J., VOLEVECKÝ, P. *Trestně právní ochrana před kybernetickou kriminalitou.* Praha : Policejní akademie ČR, 2013. s. 10. ISBN 978-80-7251-402-1.

poskytující jeho uživatelům neomezené možnosti propojení napříč planetou. Technicky se jedná o celosvětovou počítačovou síť složenou z jednotlivých menších sítí, které navzájem propojuje pomocí protokolů IP *(Internet Protocol)* a tím umožňuje komunikaci, přenos dat a informací a poskytování služeb mezi subjekty navzájem. Tím vlastně vytváří dynamický, neustále se měnící a vyvíjející systém vázaný na hardware, avšak zároveň vytvářející těžko definovatelný a prakticky neomezený kyberprostor, nemající konec ani začátek.[2]

Široká veřejnost k získání informací převážně využívá služeb nejfrekventovanějšího internetového vyhledávače Google. Tyto standardní služby tvořící tzv. *Surface web*, obnáší však pouze 4% z celkové kapacity kyberprostoru. Zbývajících 96%, tzv. *Darknet* je běžným uživatelům skryto. Při pomyslném grafickém rozdělení kyberprostoru na vrstvy zaujímá hlubší a temnější část, jak již samotný název napovídá. Připojení na Darknet probíhá přes vybrané prohlížeče (Tor, I2P, Freenet) je anonymní a komunikace šifrovaná. Samotný Darknet se pak dělí na dvě části. První, tzv. *Deep Web,* slouží své původní myšlence, tedy pro bezpečnou, necenzurovanou komunikaci a uchování citlivých dat různých institucí a to až na strategické úrovni. Druhá část, tzv. *Dark Web,* je spojena s nelegálními aktivitami. Zde se dorozumívá podsvětí, zde je možné objednat a formou kryptoměny zakoupit prakticky cokoliv. Jednou z mnoha nabízených komodit je i škodlivý software, nebo údaje platebních karet.

Pachatelem protiprávních jednání prostřednictvím Internetu, **kybernetického útoku** (*Cyber Attack*), může být jedinec, organizovaná skupina, teroristé, v krajním případě útoky mohou být iniciovány jiným státem. Jejich motivace je různá, cíl však jasný: prolomení bezpečnosti počítačových sítí se snahou narušit či omezit funkčnost jiného počítače, či získat citlivá data. Kolouch[3] definuje kybernetický útok jako jakékoli protiprávní jednání útočníka v kyberprostoru, které směřuje proti zájmům jiné osoby. Tato jednání nemusí mít vždy podobu trestného činu, podstatné je, že narušují běžný způsob života poškozeného. Podle výkladového slovníku[4] je kybernetickým útokem útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky

[2] KOLOUCH, J., VOLEVECKÝ, P. *Trestně právní ochrana před kybernetickou kriminalitou*, Praha : Policejní akademie ČR, 2013. s. 13. ISBN 978-80-7251-402-1.
[3] KOLOUCH J., *Cybercrime.* [online] Praha : CZ.NIC, 2016. s. 55. ISBN 978-80-88168-18-8. Dostupné také z WWW: <https://knihy.nic.cz/files/edice/cybercrime.pdf>
[4] JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.* [online] Praha : Policejní akademie ČR a Česká pobočka AFCEA, 2015. s. 71. ISBN 978-80-7251-436-6. Dostupné také z WWW: <https://www.afcea.cz/wp-content/uploads/2015/03/Slovnik_v303.pdf>

důležité informace. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků.

2.1 Vymezení dalších základních pojmů

Počítač je každý programovatelný stroj, který může provést naprogramovaný seznam instrukcí a reagovat na pokyny zadávané zvnějšku, přičemž zpracovává určitá data, zadaná prostřednictvím vstupních zařízení a výsledky prezentuje pomocí výstupních zařízení.[5] Technické vybavení, neboli **hardware,** je označení pro pevné komponenty počítače. Chod a činnost těchto zařízení zajišťuje **operační systém** a **aplikační vybavení.** Nezbytnou složku počítače, **počítačový program** neboli **software**, lze charakterizovat jako ucelený souhrn instrukcí, pomocí nichž provádí počítač určitou činnost.[6] Činnost počítače spočívá ve zpracování dat vkládaných uživatelem. **Data a informace,** tyto dva pojmy jsou často chybně zaměňovány či slučovány, i když samozřejmě spolu velice úzce souvisí. Zjednodušeně řečeno, shromážděná data (údaje, fakta), ať již v číselné, textové, nebo obrazové podobě tvoří podklad pro následné počítačové zpracování do informací. Jinými slovy informace jsou zpracovaná data poskytující širší význam. **Počítačový systém** je funkční jednotka, která je složena z jednoho nebo více počítačů a přidruženého software.[7] Pod tímto pojmem si představme i další technické prostředky jako mobilní telefony, tablety, bankomaty, GPS navigace, nebo tzv. chytré spotřebiče. Aby vše spolu dokázalo komunikovat, je třeba propojit počítačový systém pomocí kabelů, telefonních linek, nebo bezdrátového spojení (Wi-Fi) a vzniká tak **počítačová síť.** Všechna zařízení připojená na Internet spolu komunikují pomocí **Internet Protocolu** *(IP)* a každé toto zařízení má přidělen svůj číselný identifikátor, **IP adresu.** Veškerá přijímaná, nebo odesílaná data přes počítačovou síť tak obsahují IP adresu odesílatele i příjemce. Podle tohoto identifikátoru lze zjistit zeměpisnou polohu používaného zařízení, ať již se jedná o počítač, tablet nebo mobilní telefon, které však může být pouze v roli hostitele. IP adresu v souvislosti s prokazatelností trestného činu Ján Matějka[8] specifikuje takto: *Jakkoliv může jít o náročnou expertní činnost, lze takový důkaz úspěšně provést, a to právě na základě*

[5] SMEJKAL, V. *Kybernetická kriminalita.* Plzeň : Aleš Čeněk, 2018. 27 s. ISBN 978-80-7380-720-7.
[6] KOLOUCH, J. *Cybercrime.* [online] Praha : CZ.NIC, 2016, s. 63. ISBN 978-80-88168-18-8. Dostupné také z WWW: <https://knihy.nic.cz/files/edice/cybercrime.pdf>
[7] KOLOUCH, J. *Cybercrime.* [online] Praha : CZ.NIC, 2016. s. 58. ISBN 978-80-88168-18-8. Dostupné také z WWW: <https://knihy.nic.cz/files/edice/cybercrime.pdf>
[8] MATEJKA, J. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí.* [online] Praha : CZ.NIC, 2013. s. 90. ISBN 978-80-904248-7-6. Dostupné z WWW: <https://knihy.nic.cz/files/edice/internet_jako_objekt_prava.pdf>

samotného kontextu v podobě dalších záznamů síťového provozu, případně na základě dalších důkazů, ze kterých vyplývá, že konkrétní fyzická osoba v předmětném čase pracovala s počítačem majícím tuto IP adresu. Ve vztahu pohybu v kyberprostoru a informačním a komunikačním technologiím je třeba definovat pojem **Internet Service Provider** (*ISP*), neboli poskytovatele internetových služeb. Tyto fyzické nebo právnické osoby umožňují koncovým uživatelům připojení do počítačových sítí, postupem doby se jejich služby rozšiřují na sociální sítě nebo poskytování cloudových úložišť. Internet Service Provider se svou vlastní činností bezprostředně podílí na jeho budovaní a obměně.[9]

2.2 Kyberprostor a právo

Prostřednictvím Internetu jsou bourány teritoria i geografické vzdálenosti. Umožňuje jednak formu komunikace, získávání informací z celého světa, ukládání dat, hojně je využíván i pro zábavu. Internet je třeba vnímat i jako střet technických, ekonomických, sociálních a kulturních aspektů. Z tohoto je patrné, že meze zákona v této oblasti jsou složité a díky profilu prostředí sporné.

Internet je charakterizován jako síť sítí, která se skládá z milionů soukromých, veřejných, akademických, obchodních a vládních sítí, s místním až globálním rozsahem, které jsou propojeny širokou škálou elektronických, bezdrátových a optických síťových technologií.[10] Tyto sítě lze označit a zařadit podle zákona č. 89/2012 Sb. Občanského zákoníku coby hmotnou věc (§ 489 „*Věc v právním smyslu je vše, co je rozdílné od osoby a slouží potřebě lidí*“).[11] Internet tedy má hmotnou podstatu v podobě jednotlivých počítačových sítí, které mají své vlastníky (právnické či fyzické osoby, nebo stát), ale jako celek tato infrastruktura majitele nemá a tudíž nemá ani právní subjektivitu. V případě protiprávních jednání, podle tuzemských zákonů a mezinárodních úmluv, nesou zodpovědnost jednotliví vlastníci této infrastruktury, poskytovatelé placených služeb a samozřejmě samotní uživatelé.

[9] KOLOUCH, J., *Cybercrime*, [online] Praha : CZ.NIC, 2016. s. 78. ISBN 978-80-88168-18-8. Dostupné také z WWW: <https://knihy.nic.cz/files/edice/cybercrime.pdf>

[10] JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.* [online] Praha : Policejní akademie ČR 2015, s. 59. ISBN 978-80-7251-436-6. Dostupné také z: WWW: <https://www.afcea.cz/wp-content/uploads/2015/03/Slovnik_v303.pdf>

[11] ČESKO. Zákon č. 89 ze dne 3. února 2012 občanský zákoník. In *Sbírka zákonů České republiky*. 2012, částka 33, s. 1026-1368. Dostupné také z WWW: <https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=89/2012&typeLaw=zakon&what=Cislo_zakona_smlouvy> ISSN 1211-1244.

2.3 Působnost práva v kyberprostoru

Trestné činy páchané v kyberprostoru mají zpravidla teritoriální přesah více území, počínaje místem útoku samotného a místem následků konče. Do stíhání pachatele se tak zapojují orgány činné v trestním řízení všech zúčastněných států. Spolupráce na této úrovni je v české legislativě stanovena zákonem č. 104/2013 Sb. o mezinárodní justiční spolupráci ve věcech trestních a umožňuje i zapojení mezinárodních organizací jako Europol nebo Interpol. Z tohoto aspektu je patrné, že bylo třeba upravit také tradiční právní koncepty a zásady kybernetickému prostředí. To se týká přizpůsobených pravidel hmotné a procesní jurisdikce, která se věnují ústřednímu problému kybernetického práva: který trestní zákon použít a orgány, kterého státu jsou příslušné stíhat kyberkriminalitu s ohledem na to, že se čin, přenos dat, nebo důsledky tohoto činu odehrávají v několika zemích najednou.[12]

2.4 Působnost trestních zákonů v ČR

České právní normy rozlišují působnost uplatnění zákona, jinými slovy okruh společenských vztahů, podle čtyř určujících kritérií: působnosti časové, působnosti místní, působnosti věcné a působnosti osobní.

Pro oblast kybernetické kriminality je z hlediska posuzování nejvýznamnější působnost místní, kdy je vymezeno užití zákona ve vztahu k místu, kde byl trestný čin spáchán. Trestní zákoník[13] zahrnuje tyto základní principy:

- §4 *Zásada teritoriality*, kdy je posuzována trestnost činu spáchaného na území ČR, přičemž není brána v potaz státní příslušnost pachatele, ale nastaly tyto distanční delikty: pachatel se tohoto dopustil na území republiky, následky nastaly zcela nebo zčásti v cizině nebo pachatel se tohoto dopustil v cizině, následek nastal zcela nebo z části na území ČR.
- §5 *Zásada registrace,* kdy je posuzována trestnost činu, který byl spáchán mimo území našeho státu (např. na lodi, letadle s registrací v ČR). Místo spáchání takového činu se posuzuje obdobně podle § 4.
- §6 *Zásada personality,* kdy je posuzována trestnost činu, který v cizině spáchal občan ČR nebo osoba bez státní příslušnosti s povolením trvalého pobytu v ČR.

[12] ZAVRŠNIK, A. *Kyberkriminalita.* Praha : Wolters Kluwer ČR, 2017. s. 54. ISBN 978-80-7552-758-5.

[13] ČESKO. Zákon č. 40 ze dne 8. ledna 2009 trestní zákoník. In *Sbírka zákonů České republiky*. 2009, částka 11, s. 354-464. Dostupné také z WWW: <https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=40/2009&typeLaw=zakon&what=Cislo_zakona_smlouvy> ISSN 1211-1244.

- §7 *Zásada ochrany a zásada univerzality*, paragrafy v tomto odstavci posuzují trestnost činu, který v cizině spáchal cizí státní příslušník nebo osoba bez státní příslušnosti a bez povolení trvalého pobytu v ČR.
- §8 *Subsidiární zásada univerzality*, kdy je posuzována trestnost činu spáchaného v cizině cizím státním příslušníkem nebo osobou bez státní příslušnosti, která nemá na území ČR povolen trvalý pobyt, ale spáchala trestný čin ve prospěch právnické osoby sídlící na území ČR.

Česká republika je však vázána i některými mezinárodními úmluvami, jejichž jurisdikce je odlišná a na základě tohoto, podle §9 *Působnost stanovená mezinárodní smlouvou*, předchozí ustanovení místní působnosti nebudou použita. Ostatně určení soudní pravomoci v případě kybernetického trestného činu je zakotveno v Evropské úmluvě o počítačové kriminalitě,[14] článek 22, odst. 5: *Pokud více než jedna strana nárokuje pravomoc vůči údajnému trestnému činu podle této Úmluvy, zúčastněné strany se, pokud to bude vhodné, vzájemně poradí, aby určily nejvhodnější pravomoc pro trestní stíhání*, jejímž signatářem je i Česká republika. O tomto legislativním dokumentu bude následně pojednáno v kapitole 5.1.

2.5 Vznik a historie počítačové kriminality

Prvopočátkem elektrotechnické komunikace je vynález telefonního přístroje. Prostor komunikace, tedy propojení mezi dvěma linkami, dal později základy ke vzniku první komunikace i mezi dvěma počítači a vznikl tak virtuální svět, který dnes nazýváme kyberprostor. Jedná se o Síť, neidentifikovatelný prostor mezi počítači, mezi dvěma modemy, neurčitý prostor, kde se odehrává veškeré dění na síti, zábava, komunikace, obchod a samozřejmě také zločiny.[15]

V roce 1946 další zásadní moment odstartoval zrod tzv. počítačového věku, kdy na americké univerzitě byl sestrojen první elektronický počítač. Tato výpočetní technika svými prostorovými parametry a vysokou pořizovací cenou vyžadovala speciální a řádně zabezpečené umístění. Právě v tomto období se z řad programátorů rekrutují *hackeři,* kteří svými zásahy do programu zajišťovali bezchybnou funkčnost systémů. Postupem doby tento termín mění svůj význam, k čemuž v prvopočátcích, koncem šedesátých let minulého století, zásadně přispěl odpor k vietnamské válce. Disidenti,

[14] ČESKO. Sdělení ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě č. 104 ze dne 23. prosince 2013. In *Sbírka sbírka mezinárodních smluv České republiky*. 2013, částka 56, s. 10784-10838. Dostupné také z WWW: https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=104/2013&typeLaw=mezinarodni_smlouva&what=Cislo_zakona_smlouvy ISSN 1801-0393.

[15] MATĚJKA, M. *Počítačová kriminalita.* Praha : Computer Press, 2002. s. 19. ISBN 80-7226-419-2.

kteří se sdružovali pod názvem *yippies* objevili způsob, jak lze úspěšně nabourávat cizí telefonní linky, ústředny a postupně vůbec celý telekomunikační systému. Své úspěchy, tedy nelegální činnost nazvanou *phreaking,* publikovali v časopise *Youth International Party Line*. Koncem sedmdesátých let se podařil významný a zásadní krok, kdy dochází k propojení telefonní technologie s počítačem, tzv. *Bulletin Board System* (BBS). Sálové počítače byly spojovány do sítí již v letech šedesátých, ale právě vznikem první BBS získal každý majitel příslušně vybaveného počítače s telefonní linkou možnost stát se součástí kyberprostoru.[16]

Zlomem v dalším vývoji a to zcela zásadním, byl počátek osmdesátých let minulého století, kdy americká společností IBM uvedla na trh první osobní počítač. Cenová dostupnost se postupně stávala přijatelnou, což mělo za následek rozšíření nejen do firem, ale zejména do domácností. Zmíněný systém BBS (počítač-telefonní linka) pomocí modemů umožňuje propojení do sítí a vzniká tak předchůdce Internetu. Jednalo se většinou o servery s textovým rozhraním, na které se připojovalo přímo volbou čísla, zprostředkování přístupu pomocí *Internet Service Providerů* (ISP) přišlo až později.[17] Díky systému BBS vzniká hackerská skupina *„Legion of Doom"*, která byla považována za nejvlivnější a nejschopnější. Jakési sdružení, které svoji činnost nejen publikovalo v samizdatovém časopisu, ale také šířilo právě po BBS. Mimochodem v průběhu a zejména koncem dekády 80. let dochází k enormnímu nárůstu hackerských skupin. Stěžejní případ, tzv. *floridský skandál*, kdy došlo hackery k cílenému přesměrování úředních telefonních hovorů až za hranice státu a později kolaps telefonní sítě, rovněž připisovaný hackerům, zřejmě však způsobený chybou v softwaru, bylo impulsem pro razantní policejní operaci *Sundevil* v roce 1990. To vše sice vyústilo v zadržení počítačových a telekomunikačních odborníků, mnohdy velice schopných amatérů, pro které bývá nabourání se do systému výzvou, avšak kromě poškození telekomunikační společnosti nebyly ohroženy životy ani bezpečnost státu. Policejní razie měla sice odstrašující charakter, ale současně se otevřela otázka zásahu státu do oblasti ochrany svobody projevu a občanských práv v kyberprostoru. Za tímto účelem byla založena *Electronic Frontier Foundation* (EFF), jejímž úkolem je bránit cestou soudních sporů cyberspace před nežádoucí ingerencí státní moci. Ovšem i počítačová policie prošla svou cestou organizace. Vznikl FCIC, zvláštní mozkový trust všech

[16] MATĚJKA, M. *Počítačová kriminalita.* Praha : Computer Press, 2002. s. 22. ISBN 80-7226-419-2.
[17] MATĚJKA, M. *Počítačová kriminalita.* Praha: Computer Press, 2002. s. 23. ISBN 80-7226-419-2.

bezpečnostních složek USA na státní i federální úrovni, který má za úkol bojovat s počítačovými zločinci.[18]

Počátek 90. let zaznamenává profesionalizaci hackerů, kteří svými schopnostmi dokáží prolomit bezpečnostní systémy s jednoznačným cílem finančního obohacení. Paradoxem je, že řada těchto dopadených hackerů, se po vykonání trestu živí v oblasti bezpečnostního poradenství. Mezi tuto hackerskou elitu patří například Kevin Mitnick, který díky svým útokům na počítače společnosti Digital Equipment získal světové prvenství. Další, Robert Morris, vyslal do světa k infikaci počítačů virus v podobě svého vyhlášeného červa. A do třetice, Kevin Poulsen, který se naboural do rozhlasové telefonní linky a podvodně tak vyhrál automobil. Nejen počítačovým světem však otřásly zejména dva případy. První, kdy hackeři zpeněžili ilegálním migrantům ukradené přístupové kódy pro telefonní spojení. Ve druhém případě se ruští hackeři v čele s Vladimírem Levinem nabourali do systému elektronického bankovnictví Citibanky. Útok byl veden po sítích, do kterých se klienti přihlašovali pomocí modemu. Ztráta se pohybovala v řádech milionů dolarů. Další případ z poloviny 90. let nese název *Argentinský hacker*. Pachatele, který měl na svědomí prolomení zabezpečení vládních počítačů v USA, se podařilo vystopovat na základě soudně povoleného odposlechu právě až v Argentině. Následoval případ průmyslové špionáže tzv. *Procesor Intel,* kdy zaměstnanec zneužil získaná firemní data pro konkurenční společnost. Událost jasně prokazující, že největší nebezpečí většinou hrozí právě zevnitř. Na přelomu století pak kulminuje hrozba počítačových virů šířících se pomocí elektronické komunikace a to otevřením přiloženého infikovaného souboru. Mezi nejznámější patří *Melissa* a *I love you*. Další následující útoky pomocí tzv. DoS, *Denial of Service* neboli *Odepření přístupu* dokázaly zahltit a vyřadit tak z provozu významné internetové obchody nebo portály. Konec devadesátých let je zlomový pro rozmach další nelegální činnosti, počítačového pirátství. Významným mezníkem se stává dostupnost vypalovaček CD, umožňující šíření nejen nelegálního software, ale zejména filmových a hudebních děl. Možnosti Internetu, technický pokrok v podobě komprimace dat a systému počítačových sítí *Per-to-Per* (P2P) nemajících teritoriální omezení, to vše se stává zlatým dolem útočníků. Situace v České republice v porevolučním období je rovněž ve znamení distribuce nelegálního software a nahrávek. Začínají se objevovat první případy zneužití osobních údajů, nejedná se však o útoky „zvenku“, ale převážně z řad zaměstnanců.

[18] MATĚJKA, M. *Počítačová kriminalita.* Praha: Computer Press, 2002. s. 25. ISBN 80-7226-419-2.

Další protiprávní jednání, ovlivněna rozvojem informačních technologií, budou specifikována v následujících kapitolách.

3 Formy kybernetické kriminality

Trestná činnost spadající do oblasti kybernetické kriminality využívá prostředky informačních technologií. Počítač je buď použit jako nástroj k této nelegální činnosti, nebo se stává terčem tohoto útoku, kdy dochází k destrukci hardware, software, dat nebo počítačových sítí. Zde je třeba vyloučit protiprávní jednání, kdy je tato technika použita nad svůj rámec určení, stává se součástí či cílem majetkové trestné činnosti a dochází tak k naplnění skutkové podstaty krádeže či loupeže počítače včetně počítačového vybavení, coby věci movité.

V odborné literatuře je uváděno několik způsobů dělení kybernetické kriminality. Jak uvádí Matějka,[19] všechny definice se v zásadě shodují v tom, že je nutné rozlišit dvě základní kategorie:

- Protiprávní jednání směřující *proti počítači*. Počítač je zde přímo terčem útoku. Jedná se především o průniky do systémů za účelem například krádeže dat, průmyslové špionáže, bankovního podvodu, zneužití osobních údajů z elektronické databáze apod.
- Protiprávní jednání spáchaná s *využitím počítačů*. Počítač slouží pouze jako nástroj trestné činnosti, respektive jejího usnadnění. Na předním místě zde stojí porušování autorského práva, šíření pornografie a extremismu a zejména různé formy podvodných jednání.

Přičemž se jedná:

- Protiprávní jednání *tradiční*, kde počítač pouze usnadňuje jejich spáchání, ať už je přímo jejich terčem, nebo toliko jejich nástrojem.
- Protiprávní jednání *zcela nová*, která se objevila až s nástupem moderních informačních technologií, ať už směřující proti počítači (*hacking*), či používající počítač v roli nástroje (*cracking*).

Útoky v kyberprostoru se postupem doby stávají stále více sofistikovanějšími a představující hrozby dělí Jirovský[20] následovně:

- **Únik informací** je stav, kdy dojde k vyzrazení chráněné informace neautorizovanému subjektu.
- **Narušení integrity** představuje poškození, změnu či vymazání dat.

[19] MATĚJKA, M. *Počítačová kriminalita.* Praha : Computer Press, 2002. s. 6. ISBN 80-7226-419-2.
[20] JIROVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha : Grada Publishing, 2007. s. 21. ISBN 978-80-247-1561-2.

- **Potlačení služby** znamená úmyslné bránění v přístupu k informacím, aplikacím či systému.
- **Nelegitimní použití** je užití informací neautorizovaným uživatelem.

3.1 Pachatelé

Pojem *hacking* označuje neoprávněné proniknutí do systému cizího počítače nebo informačních technologií narušením jejich bezpečnostní ochrany. Pachatelé, kteří se většinou rekrutují z řad programátorů, nebo výjimečně i amatérů-nadšenců, mají vynikající znalosti software a principů fungování ať už počítačových operačních systémů, síťového připojení, nebo aplikací. Kromě příslušného technického hardwarového a softwarového vybavení, velkou roli sehrává sama osobnost útočníka. Jejich motivace je různá. Těžko odhadnout, zda na prvním místě tohoto pomyslného žebříčku je prestiž nebo finanční zisk. Kromě již zmíněného hnacím motorem může být zábava, emoce, sexuální motivace, psychická nemoc, stejně tak jako politika.

Útočníka či pachatele kybernetické kriminality lze dělit podle několika kritérií. Z pohledu, odkud jsou útoky vedeny, vede k logickému dělení na **útočníky vnější** a **vnitřní.** Vnější útočník musí překonat veškeré zabezpečovací prvky, jeho výhodou je nesnadná lokalizace, prakticky se může vyskytovat kdekoliv. Motivy vnitřního útočníka, tedy zaměstnance, mohou být různé. Získat informace pro konkurenci, sabotáž, pomsta kolegovi, některé incidenty mohou být spáchány nevědomě z nedbalosti.

Následné dělení pachatelů vychází z jejich schopností, potažmo nebezpečnosti. **Amatéři** nedisponují dostatkem znalostí ani dostatečným technickým vybavením, spíše prověřují své možnosti. Oproti tomu **hackeři** mají odpovídající znalosti a vzdělání v oboru, motivací jejich útoků je prověřování svých kvalit. Sofistikovaných a nepředvídatelných útoků s kvalitním vybavením jsou pak schopni **profesionálové**, jejichž motivací je jednoznačně finanční zisk, mohou být součástí podsvětí, stejně tak jako ve službách jiného státu.

Podle způsobu provedení, který nemusí mít vždy nutně destruktivní záměr a současně podle způsobu naložení se získanými daty lze útočníky rozdělit do následujících skupin, slangově označených jako *klobouky*:

White Hats jsou hackeři, kteří uskutečňují své průniky do systému za využití bezpečnostních slabin systému právě za účelem odhalení těchto bezpečnostních mezer a vytvoření takových mechanismů a bariér, které by tyto útoky měly znemožňovat. Jsou často zaměstnanci či externími spolupracovníky renomovaných společností

podnikajících v oblasti informačních technologií. Svým průnikem do systému nezpůsobují uživatelům škodu, naopak v mnoha případech upozorňují správce takto napadeného systému na bezpečnostní chyby. Jejich činnost je zásadně nedestruktivního charakteru.

Black Hats v podstatě opak hackerů řazených mezi White Hats. Jejich motivací je snaha způsobit uživateli napadeného systému škodu či jinou újmu, resp. získat majetkový nebo jiný prospěch. Mimo vlastní realizaci prolomení napadeného systému je v jejich jednání patrný ještě další, kriminální prvek.

Gray Hats jde o šedou zónu hackerů, tedy o osoby, které se nevyprofilovaly směrem k uvedeným dvěma skupinám.[21]

3.2 Nástroje pachatelů

Sdělovací prostředky ovlivnily laickou veřejnost natolik, že obecně vnímá označení *hacker* coby osobu narušující nebo nelegálně pronikající do počítačových sítí. Hackeři se sice pohybují na hraně zákona, avšak ctí tzv. hackerskou etiku, neškodí. Z výše uvedeného je pak patrné, že teorii *Black Hats* naplňují *crackeři,* zneužívající hackerské metody, kteří ke své činnosti využívají různých technických nástrojů:

- **prolamovače hesel** - tento nástroj určený k prolomení ochrany počítače se řadí mezi nejstarší programy. Tyto pracují na principu kombinace různých znakových, číselných či slovních variant zaměřených na cíl, resp. konkrétního uživatele
- **skenování portů** - se řadí k poměrně často používané technice, která snadno zjistí otevřené síťové porty cíleného počítače a potenciální útočník tak mapuje slabá místa pro další postup
- **backdoors** - neboli *zadní vrátka* je označení pro kódy, které po instalaci na cílový počítač umožňují jeho vzdálené řízení[22]
- **sniffery** - je označení pro nelegální programy umožňující odposlech provozu na síti, získané informace jsou pak vyhodnoceny pro potenciální útok
- **keylogger** - dalším pomocníkem je tento skrytý program, zaznamenávající veškeré údery na klávesnici. Získané informace jsou odesílány na předem určený server. Po vyhodnocení není složité zjistit kromě navštívených webových

[21] KOLOUCH, J., VOLEVECKÝ, P. *Trestně právní ochrana před kybernetickou kriminalitou.* Praha : Policejní akademie ČR, 2013. s. 51. ISBN 978-80-7251-402-1.
[22] JIROVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha : Grada Publishing, 2007. s. 63. ISBN 978-80-247-1561-2.

stránek, či osobních nebo jinak důvěrných informací i přístupová hesla nebo při internetové platbě čísla platební karty

- **rootkity** - představují systém počítačových programů, jejichž technologie umožňuje v napadeném počítačovém systému upravit buď jádro operačního systému, nebo uspořádat nadstavbové aplikace a tak maskovat přítomnost virů. Jejich odhalení je velice náročné, speciální antivirový program musí prohledat v systémové paměti všechny související procesy
- **botnet –** je soubor počítačů, které byly infikovány červem nebo trojským koněm instalujícím kód (známý jako bot). Ten útočníkovi umožňuje spouštět vzdálené příkazy a používat systémy pro budoucí útoky. Kód malwaru otvírá zadní vrátka, která hackerovi umožňují ovládat stroj a vzdáleně provádět příkazy.[23]

3.3 Útoky

Převážná část protiprávních jednání páchaných prostřednictvím Internetu zahrnuje tradiční skutkové podstaty, jen forma provedení je jiná. Pachatel, resp. umístění jeho počítače je velmi těžko identifikovatelné. Ač mohou být útoky vedeny z pohodlí domova, cíleny jsou přes několik internetových serverů. Anonymitě rovněž nahrává možnost využití veřejně dostupných počítačů a bezdrátového připojení. Útočníci, vesměs profesionálové, často v dobře organizovaných skupinách, využívají zejména minimální gramotnosti uživatelů a jejich závislosti na Internetu. Jejich profit je nedozírný. Škála a variabilita kybernetických útoků je velice široká. Proto pro naše účely budou specifikovány pouze nejzávažnější, nebo nejfrekventovanější.

3.3.1 Sociální inženýrství

Tento společenskovědní obor nazývaný též *umění klamu*, zahrnuje psychologickou manipulaci a opírá se o myšlenku, že nejslabším článkem řetězu je a vždy bude člověk. Metoda sociálního inženýrství nespadá do kategorie přímých kybernetických útoků, ale je jedním z podpůrných a poměrně velice úspěšných nástrojů útočníka. Využívá víceméně negativních lidských vlastností jako slabost, neodpovědnost, hloupost, lenost, ale zejména důvěřivost. Technika šikovné manipulace pak ovlivní oběť natolik, že dokáže vyzradit citlivé informace, které mohou být použity nejen proti jednotlivci, ale zejména poškodit firmu či instituci. Fázi přímého kontaktu

[23] McCARTHY, L., WELDON-SIVIY, D. *Buď pánem svého prostoru.* [online] Praha : CZ.NIC, 2013. s. 55. ISBN 978-80-904248-6-9. Dostupné také z WWW: <https://knihy.nic.cz/#bud_panem>

předchází sběr údajů a informací o potenciálním cíli. K omezení rizik a následků sociálního inženýrství patří jednoznačně povědomí o tomto nebezpečí a obezřetnost, ve firmách pak důkladné proškolení zaměstnanců.

3.3.2 Podvod a zpronevěra

Trestné činy podvodu a zpronevěry, podvodné aktivity za účelem získání finančních prostředků na úkor druhých, se sice řadí mezi tradiční jednání, avšak s používáním počítačů a rozmachem Internetu získaly nové možnosti. Obvykle se jedná o nabídku velmi levného a předem hrazeného zboží, nebo služby prostřednictvím důvěryhodně působícího e-shopu, který klame fiktivními recenzemi spokojených zákazníků, čímž je ovlivněno jednání další potenciální oběti. Pachatelům nahrává i rostoucí oblíbenost nákupů přes Internet.

3.3.3 Padělání

Dalším tradičním trestným činem, který využívá počítač coby úspěšný nástroj k této činnosti, jsou padělky, ať již se jedná o různé dokumenty, osobní nebo cestovní doklady, vysvědčení, nebo jiné veřejné listiny, především pak bankovky. Pro potírání těchto protiprávních jednání je proto využíváno metod aplikace viditelných ochranných markantů na tyto paděláním ohrožené prvky. Zejména u bankovek je mnoho možností zabezpečení, kdy se jedná např. o vodoznak, okénkový proužek s mikrotextem, barevné vlákno, skrytý obrazec ap.

3.3.4 Průmyslová špionáž

Průmyslová špionáž, nelegální sběr informací o konkurenci, patří k nejstarším protiprávním jednáním a v současné době se řadí k nejnebezpečnějším. Zahrnují různé fyzické metody, které lze označit za klasické, avšak tato aktivita s rozšířením počítačů a Internetu získala nový rozměr. Ovlivňují nejen ekonomiku, ale i politiku, mohou se tak stát ohrožením civilizace. Středem zájmu jsou významné konkurenční skutečnosti, zejména výzkumy, nové výrobky a know-how. Způsobené škody bývají nedozírné, mnohdy mohou být i likvidační.

3.3.5 Phreaking

Phreaking má dlouhou a bohatou historii a vždy byl úzce spojen s počítačovým undergroundem a hackingem.[24] Činnost phreakera, jejíž počátky jsou zmapovány již v

[24] MATĚJKA, M. *Počítačová kriminalita.* Praha : Computer Press, 2002. s. 72. ISBN 80-7226-419-2.

60. letech minulého století, spočívá v nabourání se do cizí telefonní linky. Pro tyto telefandy byla určitým druhem zábavy. Užitkem pro pachatele bylo volání na účet nic netušícího majitele telefonní linky. Postupem doby technika phreakingu umožňovala i odposlouchávání telefonních hovorů k získání citlivých informací. Tato nelegální činnost vrcholila v počátcích Internetu, kdy byly používány dnes již zastaralé modemové linky.

3.3.6 Carding

Používání platebních karet, umožňující bezhotovostní transakce, se stalo součástí běžného života většiny populace. Pojem *carding* označuje protiprávní jednání, které nabralo na intenzitě s rozvojem internetového obchodu, probíhá několika způsoby a na svědomí je mají dobře organizované skupiny, kdy cíl je jasný: odčerpání finančních prostředků z bankovních účtů, v tomto případě přes získaná data z platebních karet.

V počátcích, kdy veřejnost neměla povědomí o postupech komunikace bankovních ústavů se svými klienty, stačilo obratným pachatelům telefonicky použít metodu sociálního inženýrství. Klient tak sám vyzradil důvěrné informace. S následným rozvojem plateb přes Internet se objevují další způsoby. Sofistikovanější metody označované *Card Skimming* kopírují přístupové kódy přes tzv. čtečku karet, která je nainstalována do bankomatu a umožňuje zaznamenat údaj z magnetického proužku. Zaznamenány byly i případy, kdy do bankomatu byla instalována kamera k zachycení PINu. Na základě takto elektronicky získaných informací je vyroben padělek platební karty.

3.3.7 Spamming

Tímto pojmem je označováno masové šíření nevyžádané zprávy prostřednictvím elektronické pošty, kdy se zejména jedná o reklamní sdělení. Charakteristickým znakem tohoto jednání je hromadné rozesílání. Tyto nevyžádané, pro příjemce převážně obtěžující zprávy, které zasahují nejen do e-mailové komunikace, ale i do dalších forem internetové komunikace, např. diskusních fór nebo sociálních sítí a ve většině případů ji zcela zahlcují, však mohou být i současně nositeli virů. V současné době jsou k dispozici programy, které dokáží tyto zprávy filtrovat. Trestně právní postih tohoto jednání v České republice není zcela vyřešen, protože toto jednání je těžko zařaditelné.

Určitou formou spamu je rovněž elektronickou cestou šířící se tzv. **hoaxes,** jejichž úkolem je zasáhnout emoce příjemce, či vyvolat paniku. Obsahují různá falešná varování před smyšlenými viry, nebo výzvy, žádosti či prapodivné příběhy (tzv. **Urban**

Legends) a podle Matějky[25] zprávy tohoto druhu mají široký záběr a dokáží skutečně ovlivnit chování mnoha uživatelů Internetu.

3.3.8 Phishing

Podvodná metoda, usilující o zcizování digitální identity uživatele, jeho přihlašovacích jmen, hesel, čísel bankovních karet a účtu za účelem jejich následného zneužití.[26] Principem tohoto útoku je e-mailové rozesílání podvodného sdělení, jehož součástí je odkaz na webovou stránku, která je velmi zdařilou napodobeninou originálu např. bankovního ústavu, nebo společností zabývajícími se elektronickým převodem finančních prostředků při internetových nákupech. Adresát je vyzván v rámci „zabezpečení" přístupu ke sdělení svých přihlašovacích údajů. Tyto útoky naplňují skutkové podstaty trestného činu podvodu či padělání.

Další formou phishingového útoku je tzv. *Spear-phishing* zpravidla namířený proti předem vytipovanému příjemci, obvykle organizaci. Kromě finanční motivace pachatele, nebo získání citlivých dat bývá cílem poškození společnosti. Útočníkem bývá důvěryhodná osoba, nebo organizace, jehož adresa nefiguruje na žádném blacklistu. Mail obsahuje přílohu se škodlivým kódem, jež antivirový program nedetekuje. Po otevření přílohy tento kód shromažďuje data, která rozesílá do kyberprostoru.

3.3.9 Pharming

Nebezpečnost tohoto sofistikovaného útoku spočívá v průniku pachatele na DNS server (*Domain Name Systems*), kdy v prohlížeči dochází k přiřazení doménového jména (např. banky) s číselnou IP adresou, pomocí čehož je usnadněna komunikace všech zařízení v Internetu. Útočník pak nadefinuje svou falešnou IP adresu, přičemž uživatel je přesměrován na podvržené, obvykle těžko rozpoznatelné webové stránky bankovního ústavu. Další možností je napadení koncového uživatele počítače a to alternativní úpravou souboru Hosts.

3.3.10 Sniffing

Označuje specifickou metodu nelegálního odposlechu síťové komunikace, kterou umožňuje nezašifrování elektronických zpráv. Prakticky se jedná o počítačový program zachycující pakety a zaznamenávající komunikaci v počítačové síti. Obvykle

[25] MATĚJKA, M. *Počítačová kriminalita.* Praha : Computer Press, 2002. s. 68. ISBN 80-7226-419-2.
[26] JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.* [online] Praha : Policejní akademie ČR a Česká pobočka AFCEA, 2015. s. 71. ISBN 978-80-7251-436-6. Dostupné také z WWW: <https://www.afcea.cz/wp-content/uploads/2015/03/Slovnik_v303.pdf>

se sniffery využívají k diagnostice problémů, v opačném případě jsou nástrojem pro narušení bezpečnosti. Útočník nemusí být vždy nutně „zvenku“, ale například v rámci organizace může být činnost pracovníka sledována administrátorem, pro kterého je vcelku jednoduché monitorovat e-mailovou korespondenci.

3.3.11 Malware

Tímto pojmem je označován zkráceně z počátečních písmem z anglického *malicious software* škodlivý program, jehož snahou je infikace počítače nebo jiného mobilního zařízení. Díky tomuto se daří útočníkům získat například přístupová hesla, osobní údaje či finanční prostředky. Nejznámější odrůdou je počítačový virus, který potřebuje k šíření a životu hostitele, oproti jiným formám škodlivého software.[27] Systém je zahlcen, zpomalen, postupně dochází ke změně či destrukci dat. Jedním z těchto virů s označením **ransomware** (z anglického *ransom software*), neboli vyděračský vir, je program blokující nebo šifrující data uživatele, za jejichž zprovoznění útočník požaduje výkupné.

Další skupinou jsou **počítačové červi** představující jednu z největších hrozeb prostřednictvím samostatného a automatického rozesílání sebe sama uživatelům síťové komunikace, což může vést až k zahlcení počítačové sítě a tím i celé infrastruktury. Na rozdíl od virů jsou tyto programy schopny analyzovat bezpečnostní slabiny v zabezpečení napadeného informačního systému, proto bývají taktéž využívány k vyhledávání bezpečnostních mezer v systémech nebo poštovních programech.[28]

Za velmi nebezpečné jsou právem považovány tzv. **trojské koně,** které se pro uživatele jeví zpočátku i užitečně (systém pro pamatování PINů a hesel). Pracují na principu připojení ke zcela neškodnému programu, který si uživatel volně stáhne. Spuštěním této aplikace, například spořiče obrazovky, hry nebo infikovaného souboru s obrázky či zvuky jsou bez vědomí uživatele aktivovány funkce, které umožní útočníkovi na dálku ovládat zasažený počítač. Sleduje tak jeho činnost s možností sběru dat, kdy v krajním případě získává i přístupové kódy k internetovému bankovnictví.

3.3.12 Spyware

Stejně tak jako trojský kůň i spyware neboli *špionážní software*, bývá součástí volně stažených a jinak zcela bezpečných programů, tedy opět „pracuje“ bez vědomí

[27] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat.* Brno : Computer Press, 2004. 128 s., ISBN 80-251-0106-1.
[28] KOLOUCH, J., VOLEVECKÝ, P. *Trestně právní ochrana před kybernetickou kriminalitou.* Praha : Policejní akademie ČR, 2013. s. 43. ISBN 978-80-7251-402-1.

uživatele cíleného počítače. Svá zjištění tyto programy průběžně (např. při každém spuštění) zasílají subjektu, který program vytvořil, resp. distribuoval.[29] Útočník tak získává přehledné informace o historii navštívených webových stránek. Nemusí se však jednat jen o získání podkladů pro cílenou reklamu na osobu uživatele, ale rovněž jsou ohrožena data osobního charakteru, jako například přístupová hesla. Charakteristické pro spyware je fakt, že v počítači přetrvává i po přeinstalaci systému a pro jejich nalezení jsou třeba speciální antivirové programy.

3.3.13 Adware

Tento software, obecně označován jako program podporující reklamu (z anglického *advertising supported software*), neustále obtěžuje uživatele počítače a znepříjemňuje práci zobrazováním propagačních sdělení v prohlížeči webových stránek. Mimo této viditelné a neškodné činnosti však může mít i rizikovou formu: sleduje a uchovává údaje jako je IP adresa, historie zobrazovaných stránek nebo hesla. Obvykle je opět získán z volně stažených programů.

3.3.14 DoS, DDoS útoky

Z anglického *Denial of Service* lze zkratku přeložit jako potlačení služby a jak už sám název napovídá, cílem ataků je zahlcení a následné zpomalení systému, které vede k jeho zablokování, nikoliv k destrukci. Zejména se jedná o tyto základní metody:

- zahlcení odesíláním paketů z více strojů (tzv. DDoS útok - *Distributed Denial of Service*) Při tomto druhu útoku jsou na cílový počítač směrovány pakety z mnoha dalších počítačů, načež dochází k zahlcení cílového počítače. K tomuto útoku jsou využívány též botnety.
- zahlcení příkazem ping (*Ping Flood*), kdy pomocí protokolu ICMP (*Internet Control Message Protocol*) a nástroje PING (*Packet Internet Groper*) je možné příkazem „ping“ zjistit existenci počítače s danou IP adresou a detekci času odezvy takového počítače. Jestliže je na adresu sítě zaslaný tento příkaz s podvrženou adresou cílového počítače, všechny počítače sítě odpovídají na tento příkaz právě cílovému počítači. Při opakování příkazu „ping“ pak dochází k zahlcení takového počítače.

[29] JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.* [online] Praha : Policejní akademie ČR a Česká pobočka AFCEA, 2015. s. 111. ISBN 978-80-7251-436-6. Dostupné také z WWW: <https://www.afcea.cz/wp-content/uploads/2015/03/Slovnik_v303.pdf>

- zahlcení volných systémových prostředků (*SYN-Flood*) Zasláním SYN paketů (pakety s žádostí o připojení s fingovanou hlavičkou odesílatele na cílový počítač dojde k odpovědi na tuto žádost cílovým počítačem k rezervaci systémových prostředků pro potřeby chystaného připojení. Následuje pokus o navázání spojení s dotazujícím počítačem, přičemž tato snaha o spojení může trvat i několik minut. Při zaslání více podvržených SYN paketů může dojít k zahlcení celého počítače.[30]

3.3.15 Cybersquatting

Jak již samotný termín napovídá, jedná se o nelegální obsazení, v tomto případě vytipované internetové domény. K těmto aktivitám docházelo zejména v počátcích rozmachu, resp. vstupu na Internet. Pachatel oficiálně zaregistroval doménové jméno obecně známého subjektu za účelem jeho výhodného odprodeje dané organizaci či instituci. V opačném případě doména mohla být zneužita k šíření reklam či přesměrování na pornografické stránky. V České republice v roce 2004 byla ustanovena pravidla k registraci doménových jmen. Současné dostatečné právní ošetření umožňuje pachatele stíhat za trestný čin vydírání nebo porušení práv k ochranné známce.

3.3.16 Internetové pirátství

Je označením pro nejrozšířenější formu kybernetické kriminality, kdy se útočníkům daří obejít ochranné prvky znemožňující vytvoření nelegálních kopií. Jedná se tak o porušování autorského práva ať již v oblasti programového vybavení počítače nebo hudebních či filmových děl.

Mezi nejběžnější projevy porušování autorských práv patří:

- rozšiřování díla pomocí výměnných počítačových sítí P2P (*peer-to-peer*)
- rozšiřování díla nahráváním na specializovaný server, odkud je možné volně dané dílo stáhnout
- rozšiřování díla pomocí datových nosičů přímo mezi uživateli (půjčování a následné okopírování z dat z DVD, HDD, prodej datových nosičů ap.)
- pořízení záznamu přímo při produkci a její následné rozšíření
- neoprávněné projekce audiovizuálních děl
- již vlastní obstarání si počítačového díla; počítačový program požívá zvláštní ochrany a není možné bez souhlasu nositelů autorských práv ve smyslu

[30] KOLOUCH, J., VOLEVECKÝ, P. *Trestně právní ochrana před kybernetickou kriminalitou.* Praha : Policejní akademie ČR, 2013. s. 47-48. ISBN 978-80-7251-402-1

autorského zákona pořizovat rozmnoženiny takového díla a to ani pro vlastní potřebu

- užívání počítačového programu v rozporu s licencí
- zásahy do počítačových programů s cílem překonat technická opatření nositele autorských práv zabraňujících pořizování kopií takto chráněných programů.[31]

3.3.17 Warez

Warez je slangové označení pro určitou formu počítačového pirátství. Zatímco do nástupu warezu se jednalo o izolované obory pirátství v oblasti SW, hudby a videa, díky rychlé přenosové kapacitě Internetu a stále se zdokonalujícím kompresním formátům dat spolu se zařízeními pro jejich uchování se dnes spojují všechny tyto tři činnosti do jedné.[32] Warezovou komunitu, neboli warezovou scénu, tvoří velmi dobře organizovaná skupina s přísnými pravidly, jejímž cílem není ekonomický prospěch, ale prestiž. Samotní členové se osobně neznají a dělí se na týmy, které mají svoji specializaci vždy na určitý druh produktu. V rozporu s autorským právem jsou tak raketově šířeny nelegální produkty různého typu. Nové technologie umožňují přenos i velkého objemu dat napříč kyberprostorem a tak je otázkou několika desítek minut, kdy se pirátské kopie dostanou k uživateli ve velmi krátkém čase hned po vydání originální verze. Anonymita klientů je zajištěna proxy servery.

3.3.18 Šíření materiálu se závadným obsahem

Tato trestná činnost šířící se prostřednictvím Internetu se řadí k nejfrekventovanějším. Jedná se o distribuci materiálu **pornografické povahy** zobrazující neúctu k člověku, zachycující styk se zvířetem, zejména alarmující je pak k těmto účelům využití dítěte. Pro provozovatele pornografických webových stránek, jejichž podmínkou pro přístup je registrace a poplatek, je tento druh podnikání zlatým dolem. K tomuto obchodování jsou využívány sítě P2P (*Peer-to-Peer).*

Díky možnostem elektronické komunikace se šíří rovněž nelegální zprávy porušující normy ochrany lidských práv jako jsou **nenávistná či extremistická sdělení** diskriminující rasové, národnostní či náboženské odlišnosti, v neposlední řadě pak šíření pomluv.

[31] KOLOUCH, J., VOLEVECKÝ, P. *Trestně právní ochrana před kybernetickou kriminalitou.* Praha : Policejní akademie ČR 2013. s. 53. ISBN 978-80-7251-402-1.
[32] MATĚJKA, M. *Počítačová kriminalita.* Praha : Computer Press, 2002. s. 70. ISBN 80-7226-419-2.

3.3.19 Kyberšikana

Kybernetické útoky na sociálních sítích se řadí k fenoménům současnosti. Tento novodobý jev šikany, projev určité formy násilí, který vznikl postupem doby s používáním nových komunikačních technologií, je řazen mezi stále se vyvíjející patologické jevy, kdy jsou k dispozici velmi omezené možnosti na jejich potírání. Jedná se o cílené a opakované psychické útoky prostřednictvím sociálních sítí či mobilních telefonů na jedince, ale i skupiny s cílem poškodit, ponížit či urazit. Oběť není schopna těmto atakům zabránit nebo čelit, protože jsou anonymní. Oproti klasické, tedy fyzické šikaně, oběť nikdy nemá pocit bezpečí, protože technologie, jejímž prostřednictvím se ataky šíří, jsou všudypřítomné. Kyberšikana zůstává dlouho skryta a její odhalení je složité, neboť tomu často brání samotná oběť. Agresor bývá obvykle velmi zdatný na počítači a svoji oběť, ve většině případů spolužáka, dokáže prostřednictvím zesměšňujících videí či ztrapňujících falešných profilů dokonale zahnat do kouta. Obecně se má za to, že nejvíc obětí kyberšikany je dětských a mladistvých, ale i dospělí se stávají cílem útoků například díky svým expartnerům, kolegům či konkurenci v podnikání. Kyberšikana je neodmyslitelně spojena s agresivitou.

Co do důsledků se jedná o tyto nejzávažnější formy:

- **Kyberharašení** *(obtěžování)* zahrnuje jednosměrné útoky agresora v podobě zasílání nepřeberného množství obtěžujících SMS, nebo MMS například pomocí mobilního telefonu. Určité riziko v tomto směru představuje navazování konverzace s neznámými lidmi, která se zdá zpočátku pro dotyčného přínosem, ale postupem času se stává velmi obtěžující a ze strany oběti se ji nedaří utnout.
- **Kyberstalking** *(pronásledování)* je považována za hrubší formu kyberharašení. Představuje rovněž zasílání zpráv, které však již obsahují zastrašování a výhružky a oběť začíná mít obavu o své fyzické bezpečí. V praxi se tak děje zejména v rámci dětského kolektivu, nebo v partnerských vztazích, kdy tímto způsobem zastrašuje bývalý partner.
- **Kybergrooming** označuje chování uživatelů internetových komunikačních prostředků, kteří se snaží získat důvěru dítěte a s cílem ho zneužít, zejména sexuálně, či zneužít k nelegálním aktivitám.[33] Případná osobní schůzka může vyústit ve fyzické násilí nebo zneužití oběti k dětské pornografii či prostituci.

[33] JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.* [online] Praha : Policejní akademie ČR a Česká pobočka AFCEA, 2015. s. 69. ISBN 978-80-7251-436-6. Dostupné také z WWW: <https://www.afcea.cz/wp-content/uploads/2015/03/Slovnik_v303.pdf>

- **Sexting**, jak již samotný výraz napovídá, zahrnuje elektronické rozesílání zpráv či fotografií s intimním obsahem, poškozující určitou osobu.

3.3.20 Kyberterorismus

Nárůst a šíření terorismu je jednou z nejaktuálnějších a mimořádně nebezpečných hrozeb ohrožujících celý svět. Lze jej definovat jako nástroj k ovlivnění veřejného mínění. Jinými slovy jako plánované, promyšlené a politicky motivované násilí zaměřené proti nezúčastněným osobám, sloužící k dosažení vytčených cílů.[34] Původní ideologická motivace přerůstá do roviny nacionalistické nebo náboženské. Oproti klasické formě terorismu, která představuje použití dostupných tradičních prostředků k páchání násilí (tj. zbraní), kyberterorismus jako prostředek využívá současné technologie a Internet k zajištění rychlé informovanosti zúčastněných a maskovanému plánování akcí samotných. Skrytá propaganda pak slouží k náboru nových členů. Terčem útoku, většinou politicky motivovaného, je rozložení určité infrastruktury, nevyjímaje vojenský nebo státní sektor.

3.3.21 Kybernetické války

Kybernetická válka již není jen science-fiction. Jedná se o kybernetické útoky vedené proti počítačům a sítím jiného státu, jejichž cílem je paralyzovat kritické infrastruktury, např. zásobování vodou a energií, systémy dopravy, bankovnictví, ale i obranu státu. Vladimír Smejkal do této kategorie řadí i tzv. *asymetrické hrozby*, kdy vyspělé státy ohrožují nerovnocenní útočníci malých organizovaných skupin nebo vyšinutých jedinců ze zemí třetího světa či rozvojových zemí, kteří se dokáží zaměřit prakticky na cokoliv a technologicky silnějšího soupeře překonat využitím jeho slabých míst.[35] Kyberprostor se tak stává oblastí, na kterou je třeba pohlížet i z vojenského hlediska.

[34] MINISTERSTVO VNITRA ČR: *Definice pojmu terorismus*, [online] 29.7.2009 [cit 2019-02-26] Dostupné z: <https://www.mvcr.cz/clanek/definice-pojmu-terorismus.aspx>
[35] SMEJKAL, V. *Kybernetická kriminalita.* Plzeň : Aleš Čeněk, 2018. s. 121. ISBN 978-80-7380-720-7.

4 Problematika vyšetřování kybernetické kriminality

Vzhledem k různorodosti trestných činů z oblasti kybernetické kriminality a technickému rozvoji nelze jednoznačně specifikovat způsoby vyšetřování. Každý projev kybernetické kriminality má své určité znaky, samotné trestné činy procházejí jednotlivými fázemi a to od jeho vzniku až k dopadení pachatele, pokud se jej vůbec podaří odhalit. Postupem doby, kdy dochází k tzv. novým jednáním, jsou průběžně doplňovány další vyšetřovací metody. Obtížnost sledování projevů kyberkriminality spočívá v tom, že se odehrávají v prostředí, jenž je objektivně pouze velmi obtížně vnímatelné a umožní nám jej zase a pouze počítač.[36]

Samotný režim vyšetřování a nakládání se získanými citlivými informacemi spadá do oblasti dané zákonem, kdy je třeba brát na zřetel na ochranu soukromí Ústavou ČR, Listinou základních práv a svobod a směrnicí GDPR.

Na složitém vyšetřovacím procesu se podílí tým kriminalistů, expertů z oboru informačních technologií a přizvaných soudních znalců. Charakteristickým rysem kybernetické kriminality je její vysoká latence, proto důležitým prvkem při vyšetřování je pak nejen včasné oznámení poškozeného, ale i poskytnutí vstřícné spolupráce. Při vyšetřování stejně tak jako u jiné, tradiční trestné činnosti i v této oblasti k prvotním zdrojům informací patří zajištění stop. Kromě běžných stop, např. daktyloskopických nebo písemných, počítačové stopy obsahují pro zařazení trestného činu do oblasti kyberkriminality rozhodující důkazní informace:

- stopy na výpočetní technice včetně neoprávněných zásahů do této techniky zahrnující různé úpravy vedoucí v krajnosti ke snížení nebo vyřazení užívání přístroje
- stopy na záznamových médiích a informace uložené na nich, tzv. nosiče informací jako pevné disky, diskety, CD disky
- stopy na organizační a kancelářské technice umožňující zaznamenání a uchování digitálních informací[37]

Po oznámení poškozeného musí orgány činné v trestním řízení zejména zjistit, za jakých okolností k tomuto protiprávnímu jednání došlo a shromáždit další důkazní podklady:

[36]JIROVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha : Grada Publishing, 2007. s. 19. ISBN 978-80-247-1561-2.

[37] PORADA, V., KONRÁD, Z. *Metodika vyšetřování počítačové kriminality.* Praha : Policejní akademie ČR, 1998. s. 14. ISBN 80-85981-75-0.

- informace o vlastním útoku (zjištění zdroje útoku, struktura a délka útoku, časové rozlišení od útoku po zajištění počítačových systémů a rozsah škody tímto útokem způsobené),
- informace o počítačovém systému (způsob připojení, koncové připojení, operační systém a software),
- informace o datech (povaha napadených dat, obsah paměťových médií) a jsou-li dostupné informace o pachateli, např. motiv a dostupný rozsah jeho znalostí ICT. Ve firmách je pak zásadní zjištění nastavení přístupových oprávnění k počítačovým systémům a datům.

Následky trestných činů mohou být patrné až po nějaké době, což nahrává útočníkům. Ke zjištění, identifikaci a dešifrování digitálních stop je kromě odborníků zapotřebí kvalitní a finančně náročný software. Digitální stopy jsou objemné, značně dynamické a mohou být rozptýleny na velkém geografickém prostoru a jejich životnost může být krátká.[38] Tato definice velice stručně vysvětluje, čím a proč je značně snížena objasnitelnost protiprávních jednání v kyberprostoru.

Vyšetřování se liší podle klasifikace způsobu spáchání protiprávního jednání a podle rozsahu útoku. Lehčí incidenty, jejichž náprava spadá do kompetence vedoucího pracovníka, nebo administrátora IT, nejsou ve většině případů oznámeny. V případě incidentu přímo ohrožujícího majitele ICT je již třeba sestavení vyšetřovacího týmu. Nejzávažnější incidenty pak vyžadují zapojení vyšetřovatelů a expertů z oboru, kdy po celkové analýze situace a sběru informací je určen další postup.

Odhalováním trestných činů, jejichž terčem jsou zmíněné informační systémy kritické infrastruktury a jejichž následky by mohly být fatální, se zabývá útvar Policie ČR s celostátní působností Národní centrála proti organizovanému zločinu služby kriminální policie a vyšetřování (NCOZ SKPV), jejíž sekce kybernetické kriminality je taktéž Národním kontaktním bodem pro kybernetickou kriminalitu dle Budapešťské úmluvy o kybernetické kriminalitě. Současně zajišťuje přijímání podnětů z Národního úřadu pro kybernetickou a informační bezpečnost. Spolupracuje s Interpolem a Europolem na přijímání poznatků vztahujících se k šíření dětské pornografie na Internetu.[39]

[38] JÍROVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha : Grada Publishing, 2007. s. 63. ISBN 978-80-247-1561-2.
[39] POLICIE ČR. *Národní centrála proti organizovanému zločinu. Zpráva o činnosti NCOZ* [online] 5.12.2018 [cit. 2019-03-19] Dostupné z: <https://www.policie.cz/vyhodnoceni-cinnosti.aspx>

5 Právní předpisy vztahující se ke kybernetické kriminalitě a kybernetické bezpečnosti

Snahy o potírání negativních aktivit v kyberprostoru jsou patrné od samotného rozmachu Internetu, tedy počátkem devadesátých let dvacátého století a to na mezinárodní úrovni dokumentem *Manuál OSN o prevenci a kontrole trestných činů spojených s počítači*. Ministerstvo vnitra ČR na základě analýz reagovalo na nutnost systémového boje proti počínajícímu rozmachu této formy trestné činnosti vydáním *Koncepce boje proti trestné činnosti v oblasti informačních technologií včetně Harmonogramu opatření*.[40]

K významným krokům definujícím další postupy ze strany státu je řazen vládou schválený dokument z roku 2004 *Státní informační a komunikační politika e-Česko 2006,* na který o rok později navazuje *Národní strategie informační bezpečnosti ČR* a *Národní akční plán boje proti terorismu.* V roce 2008 reakcí na narůstající kybernetické hrozby a trestnou činnost v oblasti kyberkriminality byla vydána *Koncepce boje proti organizovanému zločinu*, nahrazující původní dokument. Dne 19. října 2011 je vládním usnesením ustanoven *Národní bezpečnostní úřad,* coby gestor problematiky kybernetické bezpečnosti a zároveň coby národní autorita pro tuto oblast, následně je zřízena *Rada pro kybernetickou bezpečnost* a další součástí NBÚ se stává schválené *Národní centrum kybernetické bezpečnosti*.[41]

Dlouhodobé záměry byly státem vytýčeny a následně přijaty *Strategií pro oblast kybernetické bezpečnosti České republiky na období let 2011 až 2015,* která mimo jiné obsahovala nutnost vytvořit legislativu v rámci státu a koordinovat spolupráci v rámci evropské kybernetické bezpečnosti. Klíčovým bylo zřízení vládního CERT (*Computer Emergency Response Team*), koordinačního místa s polem působnosti řešení kybernetických incidentů, nebo jejich předcházení v případě podezření.

Počátkem roku 2015 vstupuje v účinnost zásadní zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, na jehož přípravě se podíleli zejména zástupci Ministerstva vnitra, Ministerstva obrany a Českého telekomunikačního úřadu. Připomínkování návrhu se zúčastnila i odborná veřejnost, což je na naše poměry výjimečný jev.

---

[40] MINISTERSTVO VNITRA ČR. *Koncepce boje proti trestné činnosti v oblasti informačních technologií včetně Harmonogramu opatření.* [online] [cit. 2019-03-15]. Dostupné z WWW: <http://www.mvcr.cz/soubor/koncepce-pdf.aspx>

[41] KOLOUCH, J., BAŠTA, P. a kol. *Cybersecurity.* [online] Praha : CZ.NIC, 2019. s. 88-90. ISBN 978-80-88168-34-8. Dostupné také z WWW: <https://knihy.nic.cz/files/edice/cybersecurity.pdf >

Další priority pro eliminaci rizik a hrozeb v této oblasti jsou stanoveny *Národní strategií kybernetické bezpečnosti České republiky na období let 2015 až 2020,* kdy je zřejmé úsilí státu zajistit kybernetickou bezpečnost klíčových prvků a služeb, na nichž jsou stát, organizace či uživatelé přímo závislí a zároveň snaha o zvyšování obecného povědomí o kybernetických útocích, kybernetické bezpečnosti, právech a povinnostech jednotlivých dotčených subjektů i běžných uživatelů.[42]

Počátkem srpna r. 2017 vstupuje v účinnost zákon č. 205/2017 Sb., novelizující zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů, na jehož základě vzniká *Národní úřad pro kybernetickou a informační bezpečnost* (NÚKIB), který je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany.[43]

5.1 Evropská Úmluva o počítačové kriminalitě

K efektivnímu potírání kybernetické kriminality a z tohoto vyplývající snaze o soulad právních regulací v jednotlivých členských státech Evropské Unie bylo doposud schváleno velké množství směrnic, nařízení a rozhodnutí.

K nejvýznamnějšímu mezinárodnímu dokumentu Rady Evropy, vzhledem k jeho ojedinělosti, je řazena Úmluva o počítačové kriminalitě (takto zní oficiální název dokumentu předloženého Parlamentem ČR ke schválení). Dokumentu, který byl otevřen k podpisu v roce 2001 v Budapešti, předcházela několikaletá spolupráce expertů z několika odvětví nejen z Evropy, ale i USA, Kanady a Japonska. Česká republika tuto Úmluvu podepsala 9. února 2005, s následnou ratifikací o osm let později, 22. srpna 2013.[44]

Stěžejním záměrem této Úmluvy byla harmonizace právní úpravy, resp. skutkových podstat trestných činů páchaných v kyberprostoru a stanovení standardů společného a jednotného postupu zúčastněných stran při stíhání pachatele bez ohledu na místo, kde byl trestný čin spáchán. Pro účinné potírání kybernetické kriminality v mezinárodním měřítku je řešena nejen oblast vyšetřovacích metod a pravomocí, ale rovněž otázka procesního práva.

[42] KOLOUCH, J., BAŠTA, P. a kol. *Cybersecurity.* [online] Praha : CZ.NIC, 2019. s. 94. ISBN 978-80-88168-34-8. Dostupné také z WWW: <https://knihy.nic.cz/files/edice/cybersecurity.pdf>
[43] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST: O NÚKIB [online] [cit. 2019-04-27] Dostupné z WWW: <https://www.nukib.cz/cs/o-nukib/>
[44] KOLOUCH, J., *Cybercrime*, [online] Praha : CZ.NIC, 2016. s. 332. ISBN 978-80-88168-18-8. Dostupné také z WWW: <https://knihy.nic.cz/files/edice/cybercrime.pdf>

Pro signatáře z tohoto vyplynula implementace definic určitých skutkových podstat do vnitrostátních trestných zákonů, které jsou specifikovány v kapitole II Úmluvy[45] a podle kritérií rozděleny takto:

1. Trestné činy proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů (nezákonný přístup, nezákonný odposlech, zasahování do dat, zasahování do systému, zneužívání zařízení)
2. Trestné činy související s počítačem (počítačové padělání, počítačový podvod)
3. Trestné činy související s obsahem (trestné činy související s dětskou pornografií)
4. Trestné činy týkající se porušení autorského práva a práv souvisejících s právem autorským

Pokud by legislativa členské země nebyla v souladu s Úmluvou, režim určuje tento mezinárodní dokument. Doplňujícím dokumentem k Úmluvě je Dodatkový protokol Rady Evropy č. 189, který stanoví opatření na vnitrostátní úrovni v oblasti potírání činů rasistické a xenofobní povahy páchaných prostřednictvím počítačových systémů a současně harmonizuje pole hmotného trestního práva. Dokument byl podepsán 17. května 2013 a ratifikován 7. srpna 2014.[46]

5.2 Kyberkriminalita a trestní zákoník

Samotný proces legislativy je poměrně zdlouhavý a tak není v možnostech zákonodárců společně s odborníky z oboru informatiky adekvátně reagovat na tzv. nová jednání, jejichž jednoznačná definice je mnohdy nemožná. Právní normy tak budou vždy pokulhávat za realitou.

Současný zákon č. 40/2009 Sb. Trestní zákoník však zahrnuje trestněprávní postih takových protiprávních jednání, která naplňují skutkové podstaty trestné činnosti na tuto oblast cílící a současně vycházejí z požadavků Úmluvy. Jedná se o protiprávní jednání zařazená mezi trestné činy proti majetku, zakotvené ve zvláštní části zmíněného zákona, Hlava V:

[45] ČESKO. Sdělení ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě č. 104 ze dne 23. prosince 2013. In *Sbírka sbírka mezinárodních smluv České republiky*. 2013, částka 56, s. 10784-10838. Dostupné také z WWW: https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=104/2013&typeLaw=mezinarodni_smlouva&what=Cislo_zakona_smlouvy ISSN 1801-0393.

[46] COUNCIL OF EUROPE PORTAL. *Chart of signatures and ratifications of Treaty 189.* [online] © 2018 [cit. 2019-05-23] Dostupné z WWW: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=F6wSLE5D>

- Neoprávněný přístup k počítačovému systému a nosiči informací (§230)
- Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§231)
- Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§232)
- Porušování autorského práva (§270)
- Porušení tajemství dopravovaných zpráv (§182), přičemž toto jednání může být kvalifikováno i pod §230[47]

Vzhledem k charakteru a formám kybernetických útoků jsou v trestním zákoníku ve vztahu k ICT obsaženy i další skutkové podstaty těchto trestných činů, při nichž je počítač využit jako nástroj.

- Vydírání (§175)
- Pomluva (§184)
- Šíření pornografie (§191)
- Výroba a jiné nakládání s dětskou pornografií (§192)
- Navazování nedovolených kontaktů s dítětem (§193b)
- Podvod (§209)
- Nebezpečné pronásledování (§354)
- Hanobení národa, rasy, etnické nebo jiné skupiny osob (§355)
- Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod (§356)[48]

5.3 Legislativa ke kybernetické bezpečnosti

Snahou Evropské unie je nejen řešit problematiku kybernetické kriminality v oblasti jejího efektivního potírání, ale rovněž harmonizovat právní rámec jednotlivých členských států v oblasti kybernetické bezpečnosti. Kromě primárního dokumentu, *Listiny základních práv Evropské unie,* je toto ošetřeno v mnoha dalších směrnicích, nařízeních a rozhodnutích vydaných Evropským parlamentem a Radou EU, které

[47] POLICIE ČR. *Nejčastější projevy kybernetické kriminality s odkazem na trestní zákoník* [online] © 2019 [cit. 2019-04-27] Dostupné z WWW:<https://www.policie.cz/clanek/nejcastejsi-projevy-kyberneticke-kriminality-s-odkazem-na-trestni-zakonik.aspx>

[48] ČESKO. Zákon č. 40 ze dne 8. ledna 2009 trestní zákoník. In *Sbírka zákonů České republiky*. 2009, částka 11, s. 354-464. Dostupné také z WWW: <https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=40/2009&typeLaw=zakon&what=Cislo_zakona_smlouvy> ISSN 1211-1244

současně v mnohém prolínají do legislativy o kybernetické kriminalitě, zejména do Úmluvy o počítačové kriminalitě.

Zákony České republiky, nařízení vlády a vyhlášky týkající se bezpečnosti, jsou postupem doby, resp. technickým pokrokem v oblasti ICT, rovněž vázány na pohyb v kyberprostoru. Zákon o kybernetické bezpečnosti cílí na zvýšení bezpečnosti v kyberprostoru a především ochranu kritické infrastruktury. Vymezuje odvětví, pro které by narušení informačních systémů mohlo mít fatální dopad. Jedná se o energetiku, dopravu, bankovnictví, finanční trhy, zdravotnictví, vodní hospodářství, digitální infrastrukturu a chemický průmysl. Pro dotčené subjekty z tohoto vyplývá povinnost nastavení ochranných mechanismů, které zahrnují bezpečnostní pravidla, vedení řádné bezpečnostní dokumentace, detekce kybernetických událostí a ohlašování kybernetických incidentů. Novelizací zákonem č. 205/2017 Sb., zákonodárce reagoval na Směrnici Evropského parlamentu a Rady (EU) o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.[49] Obsah této právní normy následně upřesnil prováděcí předpis *Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat.*

5.4 Informační bezpečnost

Bezpečnostní pravidla a doporučení vyplývající ze zákona o kybernetické bezpečnosti jsou pro organizace standardizovány prostřednictvím normy vydané mezinárodní společností International Organization for Standardization, ČSN ISO/IEC 27001, pro Systém řízení bezpečnosti informací *(Information Security Management System)*, která je koncipována jak pro veřejný, tak soukromý sektor. V hlavní části normy jsou specifikovány požadavky na vybudování, zavedení, provoz, monitorování, přezkoumání, udržování, zlepšování a případnou certifikaci zdokumentovaného systému managementu bezpečnosti informací. Jsou zde specifikovány požadavky na výběr a zavedení bezpečnostních opatření chránících informační aktiva.[50]

V samotných organizacích jsou pak postupy upřesněny v interních směrnicích, kdy je metodika ochrany rozlišena podle stupňů důvěrnosti, ale také pravomocí jednotlivých zaměstnanců. Pro státní správu je tato oblast legislativně ošetřena zákonem

[49] KOLOUCH, J., BAŠTA, P. *Cybersecurity.* [online] Praha : CZ.NIC, 2019. s. 93. ISBN 978-80-88168-34-8. Dostupné také z WWW: <https://knihy.nic.cz/files/edice/cybersecurity.pdf>

[50] TECHNOR. *ČSN ISO/IEC 27001* [online] TECHNOR print, s.r.o. © 2005-2018 [cit. 2019-05-05] Dostupné z WWW: <https www.technicke-normy-csn.cz/369790-csn-iso-iec-27001_4_76533.html>

č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti, který upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon.[51]

5.5 Zásady informační bezpečnosti

Nastavení bezpečnostních pravidel a činností a jejich dodržování by mělo být v zájmu každé organizace. Vzhledem k neustálému vývoji informačních technologií a současnému nárůstu zpracovávaných informací představuje oblast informační bezpečnosti souhrn pravidel a opatření zamezujících úniku a následnému zneužití citlivých informací, ať již se jedná o data jedinců nebo organizací. Proces zabezpečení informací stojí na třech základních principech: zachování důvěrnosti, integrity a dostupnosti informací.[52]

Systém řízení informační bezpečnosti (ISMS) je soubor pravidel a opatření, po jejichž zavedení má správné a úplné informace (princip integrity) včas k dispozici ten, kdo je skutečně potřebuje (princip dostupnosti) a pouze ten, kdo je k přístupu k nim oprávněn (princip důvěrnosti). V organizační struktuře organizace musí informační bezpečnost pokrývat činnosti a spolupráci vedení, osob odpovědných za aplikační systémy, provozní služby, koncové uživatele a osoby odpovědné za jednotlivé činnosti, kdy je předpokladem nejen úzká spolupráce zúčastněných, ale i řádné znalosti.[53]

Informační bezpečnost je proces, který na základě vyhodnocení analýzy a zavedením vhodných opatření zajistí ochranu informací v digitální či listinné podobě a to po celý jejich životní cyklus. Jedná se o klíčový a prakticky neustále se vyvíjející proces k maximalizaci ochrany, který je třeba řešit komplexně a to z několika aspektů: dynamiky technologií, organizačních procesů a chování zúčastněných.

Pro minimalizaci rizika je nutná funkčnost provázaných mechanismů na několika úrovních:

---

[51] ČESKO. Zákon č. 412 ze dne 21. září 2005 o ochraně utajovaných informací a o bezpečnostní způsobilosti In *Sbírka zákonů České republiky*. 2005, částka 143, s. 7526-7576. Dostupné také z WWW: <https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=412/2005&typeLaw=zakon&what=Cislo_zakona_smlouvy> ISSN 1211-1244

[52] JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.* 3. vyd. Praha : Policejní akademie ČR a Česká pobočka AFCEA, 2015. s. 23. ISBN 978-80-7251-436-6. Dostupné také z WWW: < https://www.afcea.cz/wp-content/uploads/2015/03/Slovnik_v303.pdf>

[53] KALAMÁR, Š., POŽÁR, J. *Vybrané aspekty informační bezpečnosti.* Praha : Policejní akademie ČR, 2010. s. 50-51. ISBN 978-80-7251-339-0.

- *personální* - za vším stojí lidé, ať již se jedná o správce systémů, nebo samotné uživatele. Statisticky dokázanému vysokému bezpečnostnímu riziku z řad vlastních zaměstnanců, kteří mají znalosti o fungování vnitřního systému, je třeba předcházet řádným proškolením. Personální rovina je však ovlivněna řadou dalších faktorů, ať již se jedná o zanedbání povinnosti nebo podcenění hrozícího nebezpečí, momentální psychiku nebo životní postoj
- *fyzická* - zahrnuje ochranu prostor, kde se nacházejí hmotná aktiva a lidé, např. formou zámků, kamerového systému, protipožárního systému
- *logická* - řídí přístup k systému zpracování dat (softwarové zabezpečení)
- *komunikační* - zajišťuje ochranu počítačové sítě, která přenáší data a informace
- *administrativní* - zahrnuje dodržování standardů bezpečnostní politiky v organizacích podle vypracovaných směrnic a bezpečnostních pravidel

Organizace, která je držitelem certifikátu Systému řízení bezpečnosti informací (ISMS) podle normy ČSN ISO/IEC 27001, tak tímto nejen naplní předepsanou legislativu, ale získává na trhu i jistou konkurenční výhodu, je pro klienty zárukou řádného zabezpečení a zacházení s citlivými údaji. Certifikaci vystavují nezávislé akreditované subjekty.

5.6 Ochrana soukromí

Hrozba zneužití osobních údajů je úzce spjata s rozmachem různých forem elektronické komunikace. Podle Všeobecné deklarace lidských práv (čl. 12) se soukromí řadí k základním lidským právům: *nikdo nesmí být vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence, ani útokům na svou čest a pověst. Každý má právo na zákonnou ochranu proti takovým zásahům nebo útokům.*[54] V českém právním řádu jsou ustanovení o soukromí zakotvena v Listině základních práv a svobod z roku 1992 a následně promítnuta do Občanského zákoníku, který ošetřuje i další náležitosti soukromého charakteru.

Ochrana osobních údajů byla původně regulována zákonem č. 256/1992 Sb. a následně upravena zákonem č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů. Tento byl nahrazen Nařízením Evropského parlamentu a Rady (EU) 2016/679, které nabylo účinnosti 25. května 2018 a je všeobecně známé pod zkratkou GDPR (*General Data Protection Regulation*) a aplikovatelné nejen ve všech 28 státech

[54] OSN. *Všeobecná deklarace lidských práv*. [online] © 2015 United Nations [cit. 2019-05-05] Dostupné z WWW: <https://www.osn.cz/wp-content/uploads/UDHR_2016_CZ_web.pdf>

Evropské unie, ale i v Norsku, Islandu a Lichtenštejnsku. Cílem obecného nařízení je přizpůsobení právního rámce ochrany osobních údajů dnešní době, dosažení větší jednoty právního rámce ve všech zemích na které dopadá, posílení práv subjektů údajů a v neposlední řadě je snahou dosáhnout sjednoceného výkladu obecného nařízení a dozoru jednotlivými dozorovými úřady.[55]

Dokument stanoví rozsáhlý způsob organizace práce s osobními údaji pro jejich mnohonásobně vyšší zabezpečení. Ukládá určité metody a povinnosti při ochraně osobních údajů zpracovatelům a správcům těchto dat a naopak osobám z řad klientů nebo zaměstnanců, jejichž údaje jsou zpracovávány, na půdě Evropské unie poskytuje určitá práva. Nedodržení či porušení těchto vymezených opatření v rámci GDPR je ošetřeno poměrně vysokými pokutami.

Naproti tomu trestněprávní postih za neoprávněné nakládání s osobními údaji, resp. za *trestné činy proti právům na ochranu osobnosti, soukromí a listovního tajemství*, je ošetřeno ve zvláštní části Trestního zákoníku[56] a zahrnuje tyto skutkové podstaty:

- Neoprávněné nakládání s osobními údaji (§ 180)
- Poškození cizích práv (§ 181)
- Porušení tajemství dopravovaných zpráv (§ 182)

5.7 Přehled významných zákonů ČR

Současnou českou legislativu z pohledu bezpečnosti a ochrany před kybernetickými útoky a následně pro potírání těchto trestných činů tvoří:

- Ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů
- Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů
- Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky
- Zákon č. 141/1961 Sb., o trestním řízeni soudním
- Zákon č. 14/1993 Sb., o opatřeních na ochranu průmyslového vlastnictví

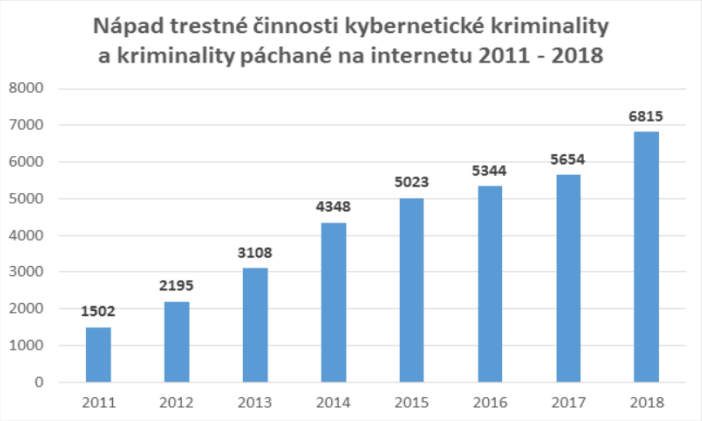
[55] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJ *Základní příručka k GDPR obecné nařízení* [online] © 2013 [cit. 2019-04-27] Dostupné z: <https://www.uoou.cz/1-obecne-na-izeni/d-27266>

[56] ČESKO. Zákon č. 40 ze dne 8. ledna 2009 trestní zákoník. In *Sbírka zákonů České republiky*. 2009, částka 11, s. 354-464. Dostupné také z WWW: <https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=40/2009&typeLaw=zakon&what=Cislo_zakona_smlouvy> ISSN 1211-1244.

- Zákon č. 160/1999 Sb., o svobodném přístupu k informacím
- Zákon č. 101/2000 Sb., o ochraně osobních údajů
- Zákon č. 121/2000 Sb., autorský zákon
- Zákon č. 240/2000 Sb., o krizovém řízení a změně některých zákonů (krizový zákon) ve znění pozdějších předpisů
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů
- Zákon č. 218/2003 Sb., zákon o soudnictví ve věcech mládeže
- Zákon č. 441/2003 Sb., o ochranných známkách
- Zákon č. 480/2004 Sb., o některých službách informační společnosti
- Zákon č. 127/2005 Sb., o elektronických komunikacích
- Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
- Zákon č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdějších předpisů
- Zákon č. 273/2008 Sb., o Policii České republiky
- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů
- Zákon č. 40/2009 Sb., trestní zákoník
- Zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů
- Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim
- Zákon č. 89/2012 Sb., občanský zákoník
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a některé další zákony
- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce
- Zákon č. 104/2017 Sb., novelizace zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů
- Zákon č. 205/2017 Sb., novelizace zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony

6 Praktické příklady

Úměrně s rostoucí závislostí populace na informačních a komunikačních technologiích se zvyšuje i riziko kybernetických útoků. Policie ČR eviduje počet nahlášených trestných činů v kyberprostoru od roku 2011, přičemž na pomyslné první příčce se drží podvodná jednání. V loňském roce pak největší nárůst zaznamenala společensky nebezpečná jednání zasahující a ohrožující výchovu z řad nezletilých a mladistvých. Zejména v oblasti výroby a šíření dětské pornografie.

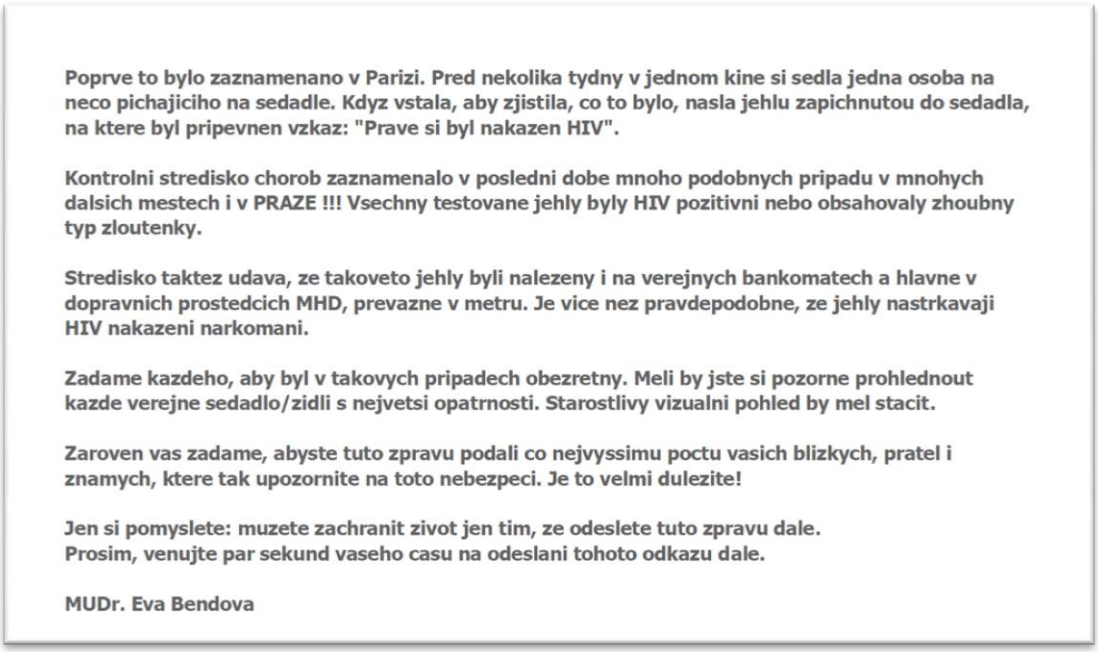


Obr. č. 1[57]

Podle Zprávy o činnosti Národní centrály proti organizovanému zločinu za rok 2018 a monitoringu protiprávních jednání v kyberprostoru v ČR lze kromě Phishingu očekávat další nárůst útoků na platební karty a bankovní účty, na různé mobilní bankovní aplikace či formou podvodných e-shopů. Lze rovněž očekávat nárůst vysoce sofistikovaných útoků na banky, DDoS útoků a ransomware.[58]

V praxi se jistě většina uživatelů setkala s určitou formou spamu, tzv. hoax, šířeným prostřednictvím e-mailu, nebo sociálních sítí. Jedná se o poplašné, varující, žertovné zprávy, polopravdy a lži. Tyto zprávy mají určité charakteristické znaky, například je kladen důraz na důvěryhodný zdroj, vyznačují se naléhavostí, šokují a hlavně vyzývají k dalšímu rozesílání. Setkat se tak můžeme s varováním před smyšlenými viry, s falešnými prosbami o pomoc, zkreslenými informacemi, řetězovými dopisy štěstí, k jejichž dalšímu masovému šíření nahrává pověrčivost samotného příjemce. Hoax nejen obtěžují, ale především zatěžují sítě.

[57] POLICIE ČR. *Kyberkriminalita.* [online]. © 2019 [cit. 2019-05-10] Dostupné z WWW: <https://www.policie.cz/clanek/kyberkriminalita.aspx>
[58] POLICIE ČR. *Zpráva o činnosti NCOZ.* [online]. 4. 12. 2018 [cit. 2019-05-10] Dostupné z WWW: <https://www.policie.cz/vyhodnoceni-cinnosti.aspx>



Poprve to bylo zaznamenano v Parizi. Pred nekolika tydny v jednom kine si sedla jedna osoba na neco pichajiciho na sedadle. Kdyz vstala, aby zjistila, co to bylo, nasla jehlu zapichnutou do sedadla, na ktere byl pripevnen vzkaz: "Prave si byl nakazen HIV".

Kontrolni stredisko chorob zaznamenalo v posledni dobe mnoho podobnych pripadu v mnohych dalsich mestech i v PRAZE !!! Vsechny testovane jehly byly HIV pozitivni nebo obsahovaly zhoubny typ zloutenky.

Stredisko taktez udava, ze takoveto jehly byli nalezeny i na verejnych bankomatech a hlavne v dopravnich prostedcich MHD, prevazne v metru. Je vice nez pravdepodobne, ze jehly nastrkavaji HIV nakazeni narkomani.

Zadame kazdeho, aby byl v takovych pripadech obezretny. Meli by jste si pozorne prohlednout kazde verejne sedadlo/zidli s nejvetsi opatrnosti. Starostlivy vizualni pohled by mel stacit.

Zaroven vas zadame, abyste tuto zpravu podali co nejvyssimu poctu vasich blizkych, pratel i znamych, ktere tak upozornite na toto nebezpeci. Je to velmi dulezite!

Jen si pomyslete: muzete zachranit zivot jen tim, ze odeslete tuto zpravu dale.
Prosim, venujte par sekund vaseho casu na odeslani tohoto odkazu dale.

MUDr. Eva Bendova

Obr. č. 2[59] *Infikované jehly na sedadlech* (první výskyt: 04/2001)

Phishingové zprávy, jak vyplývá z informací Policie ČR, se řadí rovněž k nejfrekventovanějším jevům v České republice. Podvodná technika s vysokou efektivitou k získání citlivých údajů využívající znaků sociálního inženýrství, tedy šikovné manipulace. Spočívá ve vyděšení adresáta, který koná pod momentálním stresem a panikou, proto jsou mezi postiženými často i zkušení uživatelé. K nejčastějším variantám se řadí fiktivní zprávy z bankovních domů vyzývající k přihlášení do internetového bankovnictví, kdy je po adresátovi požadována aktualizace přihlašovacích údajů, většinou s omluvou za vzniklé problémy s databází. Doručená e-mailová zpráva bývá již obvykle jazykově i gramaticky v pořádku, adresa odesílatele se jeví téměř věrohodně a tak na první pohled nevyvolává podezření. Po odkliku přiloženého linku se uživatel ocitá na podvržených, téměř autentických webových stránkách s nezabezpečeným protokolem a pokud vyplní přihlašovací údaje, útočník tak získává přístup k heslům, nebo číslům kreditních karet, které pak použije pro přímé čerpání, nebo je naopak zpeněží.

Uživatelé online bankovnictví by měli mít zažité pravidlo, že banky nikdy nezasílají svým klientům požadavky na přihlašovací údaje prostřednictvím elektronické

[59] HOAX.cz. *Infikované jehly na sedadlech.* [online]. Praha : Josef Džubák & HOAX.cz. © 2000-2019 [cit. 2019-05-10] Dostupné z WWW: http://www.hoax.cz/hoax/infikovane-jehly-na-sedadlech/>

pošty. V současné době jsou transakce internetového bankovnictví chráněny dalším zabezpečovacím prvkem, zasláním autorizačního hesla na mobil klienta, čímž je naplněna povinnost daná *směrnicí Evropského parlamentu a Rady (EU) 2015/2366 o platebních službách na vnitřním trhu*. Nicméně vynalézaví útočníci na podvržených webových stránkách nasměrují uživatele k vyplnění další zásadní informace, a sice telefonního čísla a typu telefonu. Na tento je následně zaslána SMS s odkazem na podvrženou antivirovou aplikaci, po jejíž instalaci jsou zadržovány autorizační SMS banky, které obdrží útočník a provede autorizaci ve svůj prospěch. Proto je třeba mít na zřeteli důsledné dodržování základních a poměrně logických pravidel: používat pouze vlastní počítač nebo telefon a nepřipojovat se přes free Wi-Fi sítě a kontrolovat zabezpečení domény bankovního domu (obr. č. 3).

Obr. č. 3[60]

Další zaznamenanou variantou phishingu bylo novoroční přání s infikovaným souborem, po jehož otevření se do počítače nebezpečný vir nainstaluje. Útočník tak získává přístup k počítači, potažmo k přihlašovacím údajům do banky. Dalšími podvodnými praktikami se snaží získat údaje o mobilním telefonu, na který chodí autorizační heslo, ohroženy napadením jsou zejména chytré telefony s operačním systémem Android.

Rovněž byly registrovány protiprávní aktivity na sociálních sítích. Útočník se naboural do facebookového účtu uživatele a pod jeho identitou žádá o momentální peněžní pomoc okruh jeho přátel. Tok finančních prostředků probíhá přes falešnou platební bránu, útočník tak získá informace z platební karty, nebo přístupová hesla do internetového bankovnictví. Případné kompenzaci vzniklé škody ze strany banky

[60] ČESKÁ SPOŘITELNA. *Bezpečnostní desatero*. [online]. Česká spořitelna © 2019 [cit. 2019-05-10] Dostupné z WWW: https://www.csas.cz/cs/o-nas/bezpecnost-ochrana-dat/bezpecnostni-desatero-obecna-pravidla

předchází důkladné prověření, zda nedošlo k bezpečnostnímu pochybení ze strany klienta.

V září 2018 byla veřejnost informována o vyděračských e-mailech, druhá vlna tohoto jevu následovala počátkem letošního dubna a kromě naší republiky v patřičných jazykových mutacích zřejmě obletěla celý svět. Útočníci vyhrožují zveřejněním intimních videí, která získali údajnou aplikací malware aktivujícího přední web kameru počítače, tabletu nebo mobilního telefonu a požadují výkupné ve virtuální měně. Napadení škodlivým software se nezakládalo na pravdě, ale opět útočníkům nahrálo do karet bezhlavé jednání několika zděšených příjemců. Prakticky stačilo na tyto e-maily nereagovat a odstranit je, případně označit jako spam, každopádně aktivity tohoto typu by měly být nahlášeny.

Koncem roku se v médiích objevila zpráva, kdy došlo k útokům na bankovní účty klientů prostřednictvím aplikace na nahrávání hovorů QRecorder stažené do mobilních telefonů a obsahující malware. Tímto byl útočníkům umožněn nejen přístup do internetového bankovnictví, ale současně se jim takto podařilo získat vygenerovaný autorizační kód ze zaslané SMS pro potvrzení platby, aniž by klient cokoliv tušil. Celá věc je znepokojující o to více, že infikovaná aplikace byla v nabídce oficiálního obchodu Google Play, který je obecně vnímán jako důvěryhodný zdroj.

7 Prevence v oblasti kybernetické kriminality

Účinnými preventivními opatřeními lze eliminovat kybernetické útoky a potažmo následky vzniklých škod. Prevence v rámci bezpečného užívání Internetu zahrnuje soubor opatření, které je nutné dodržovat k ochraně před únikem a zneužitím citlivých dat a informací. Státní úřady a komerční organizace mají povinnost postupovat podle Vyhlášky č. 82/2018 Sb., která stanoví bezpečnostní opatření organizačního a technického charakteru. Organizační opatření jsou nastavena interními pravidly, na tyto pak navazují technická opatření, která řeší nastavení informačních a komunikačních systémů a služeb.

7.1 Organizační opatření

Jednotlivá uzákoněná bezpečnostní opatření v organizaci zajišťuje souhrn vnitřních norem a směrnic, které specifikují obecné zásady, pokyny a metodiku práce. Dokumentaci k organizačním opatřením je třeba vypracovat na základě vyhodnocení důkladné analýzy rizik, kterými by mohl být ohrožen chod všech útvarů dotčeného subjektu. V praxi tak dochází k propojení opatření organizačních s technickými. Organizační opatření se dotýkají těchto oblastí:

- systém řízení bezpečnosti informací (aplikace komplexního procesu ISMS)
- řízení aktiv
- řízení rizik
- organizační bezpečnost
- bezpečnostní role
- řízení dodavatelů
- bezpečnost lidských zdrojů
- řízení provozu a komunikací ICT
- řízení změn ICT
- řízení přístupu ICT
- akvizici vývoj a údržbu ICT
- zvládání kybernetických bezpečnostních událostí a incidentů
- řízení kontinuity činností
- audit kybernetické bezpečnosti[61]

[61] ČESKO. Vyhláška č. 82 ze dne 21. května 2018 o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidace dat (vyhláška o kybernetické bezpečnosti). In *Sbírka zákonů České republiky.*

7.2 Technická opatření

Primárním cílem je zamezit odcizení, poškození hmotného i nehmotného majetku a úniku dat a informací. Technická opatření zahrnují zabezpečení tradičního prostředí, fyzického perimetru, propojeného s prostředím digitálním. Tento neohraničený a tudíž poměrně složitý prostor, kdy zaměstnanci se nacházejí mimo kancelář a ke své práci mohou využívat i mobilní zařízení, je logicky potenciálně zranitelnější. Fyzická ochrana v rámci objektu zahrnuje mechanické prostředky, ostrahu, kontroly vstupu, elektronický zabezpečovací systém, kamerový systém, detektory kouře, hasicí systém a záložní zdroje energie. Přísně regulovaný přístup by pak měl platit pro prostory, kde se nacházejí servery, síťové prvky, úložiště dat, nebo pracoviště administrátorů. K technickému zabezpečení ICT je třeba využít celou škálu nástrojů vrstvené ochrany, která rovněž vychází ze současné legislativy[62] a zahrnuje:

- bezpečnost komunikačních sítí (efektivní segmentace sítě, kryptografie, blokování nežádoucí komunikace)
- správu a ověřování identity uživatelů a administrátorů (identifikace a autentizace dostatečně dlouhým heslem)
- řízení přístupových oprávnění
- ochranu před škodlivým kódem (antivir s pravidelnou aktualizací)
- zaznamenávání událostí informačního systému, jeho uživatelů a administrátorů
- detekci kybernetických bezpečnostních událostí
- sběr a vyhodnocování kybernetických bezpečnostních událostí
- aplikační bezpečnost
- kryptografické prostředky
- zajišťování úrovně dostupnosti informací
- bezpečnost průmyslových a řídicích systémů

Aktuální hrozby, nebo podezření na bezpečnostní incident je třeba hlásit vládnímu nebo národnímu týmu CERT (*Computer Emergency Response Team*), které byly za tímto účelem zřízeny a kromě subjektů dotčených legislativou jsou k dispozici i

2018, částka 43, s. 1122-1168. Dostupné také z WWW: <https://www.govcert.cz/download/kii-vis/NovaVKB/VKB_82-2018sb.pdf> . ISSN 1211-1244.

[62] ČESKO. Vyhláška č. 82 ze dne 21. května 2018 o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidace dat (vyhláška o kybernetické bezpečnosti). In *Sbírka zákonů České republiky.* 2018, částka 43, s. 1122-1168. Dostupné také z WWW: <https://www.govcert.cz/download/kii-vis/NovaVKB/VKB_82-2018sb.pdf> . ISSN 1211-1244.

občanům. Na úrovni organizací takto fungují týmy CSIRT (*Computer Security Incident Response Team*).

Je třeba si uvědomit, že zajištění kybernetické bezpečnosti je nepřetržitý a neustále se vyvíjející proces, kdy stávající opatření je třeba pravidelně posuzovat a v případě nutnosti implementovat opatření nová.

7.3 Opatření v domácnosti

Domácí uživatelé ICT tvoří významně zastoupenou skupinu. Každý uživatel počítače a dalších zařízení připojených k Internetu, by měl mít v povědomí potenciální hrozby a dodržovat základní pravidla, ale prakticky tomu tak bohužel není.

K základním prvkům patří zabezpečení domácí Wi-Fi sítě dostatečně silným, originálním heslem. Pomyslná vstupní brána mezi domácí a internetovou sítí, která dokáže rozpoznat příchozí škodlivou komunikaci ze sítě, stejně tak jako ohlídat odesílání dat pouze s vědomím uživatele je nastavení firewallu. Co by mělo být samozřejmostí: legální software, aplikace stahovat pouze z ověřených zdrojů, instalace antivirového programu, případně antispyware programu. Nezbytností jsou pravidelné aktualizace antiviru a operačního systému, kdy každá nová verze poskytuje vyšší bezpečnost opravou nedostatků verze předchozí. Stejně tak by neměla být opomíjena aktualizace používaného internetového prohlížeče optimalizující stávající funkce. Pro vyhodnocení nestandardní situace i zde platí zdravý úsudek a osobní návyky: neotvírat maily s podezřelou adresou, neotvírat podezřelé přílohy a odkazy, nespouštět neznámé programy, které jsou součástí mailu, nebo na něj odkazují a kontrolovat certifikáty. Každý uživatel by měl mít v povědomí skutečnost, že všechny kroky na Internetu jsou zaznamenány formou digitální stopy, která mapuje jeho osobnost a vytváří jakousi digitální pověst. Jsou digitální stopy, které i při nejlepší vůli ovlivnit nelze (připojení k Internetu a využívající služby), ale další digitální stopy relativně ovlivnitelné jsou. Proto je na místě obezřetnost, zejména na sociálních sítích důkladně nastavit soukromí a neodhalovat o sobě víc, než je třeba.

7.4 Zabezpečení mobilního telefonu

Současné chytré mobilní telefony zasahují do každodenních činností uživatelů v mnoha směrech a jsou prakticky využívány na každém kroku. Obsahují nejen kontakty, důvěrné zprávy, fotografie, různé aplikace zaznamenávající naše aktivity, připojujeme se do on-line bankovnictví, e-mailu, jejich pomocí ovládáme různá další

zařízení (*Internet of Things*). Obecně je však jejich zabezpečení velmi podceňováno, i když většina naší komunikace probíhá právě přes připojení k Internetu a proto jsou stále více populárnější v hledáčku útočníků.

Stejně tak jako u počítačů je třeba aplikovat antivir a dbát na aktualizace operačního systému. U stahovaných aplikací je třeba sledovat požadovaná práva a přístupy, jejichž odsouhlasení by mohlo útočníkům umožnit v určitém časovém horizontu sběr důvěrných informací. Potenciální nebezpečí hrozí přes free Wi-Fi. Přes bezdrátové připojení bluetooth bychom měli stahovat data pouze z ověřených zdrojů.

Na skutečnost zanedbávání on-line zabezpečení a antivirové ochrany mobilních telefonů ostatně poukazuje i Česká bankovní asociace[63] v souvislosti s vyhodnocením Indexu bezpečnosti pro rok 2018, který dosahuje 61% a jehož hodnota je v posledních pěti letech téměř neměnná.

7.5 Osvěta

Bezpečně vstupovat do digitálního světa vyžaduje nejen uživatelské dovednosti, řádné technické zabezpečení, ale zejména ustavičné vyhodnocování on-line informací. Uživatelé Internetu již nejsou pouze konzumenty jeho obsahu, ale s rozmachem sociálních sítí se významně podílí i na růstu jeho objemu formou vkládaných fotografií, komentářů, videí apod.

Podíváme-li se kolem sebe, už malé děti v raném předškolním věku si prohlížejí pohádky na tabletu. Na jedné straně je pozoruhodné, jak se děti snadno a rychle dokáží orientovat v používání těchto prostředků, na druhé straně je alarmující potenciální vypěstování závislosti. Z tohoto faktu je patrné, jak nesporně nás ovlivňuje prostředí, ve kterém se pohybujeme a vyrůstáme, jaké máme postoje. Velkou roli s vyhodnocením on-line nebezpečí sehrávají právě generační rozdíly uživatelů a jejich návyků. Gramotnost uživatelů a to již z řad školáků je proto stěžejní pro eliminaci různých nástrah a bezpečnostních rizik. Rodiče většinou vzhledem k pracovnímu vytížení na osvětu potomků nemají mnoho času a energie, mnohdy i znalostí. Často se spíš snaží svým dětem přístup k počítači a potažmo na Internet omezovat, což však nevede k získání správných návyků a s tím spojeného vyhodnocení on-line nebezpečí. Právě sociální sítě jsou velkým rizikem, kdy děti a mladiství spadají do nejohroženější skupiny a tímto způsobem může být negativně narušena jejich psychika a zdravý vývoj.

[63] ČESKÁ BANKOVNÍ ASOCIACE: *Češi jsou nepoučitelní, nemění si hesla, nepoužívají mobilní antiviry* [online]. 22.05.2018 [cit. 2019-05-25] Dostupné z WWW: <https://www.czech-ba.cz/cs/cesi-jsou-nepoucitelni-nemeni-si-hesla-nepouzivaji-mobilni-antiviry>

Výzkumy a monitorování rizikového chování dětí a dospívajících používáním Internetu probíhá již od roku 2010. V roce 2014 Univerzita Palackého v Olomouci provedla ve spolupráci s největšími internetovými portály v ČR Seznam a Google rozsáhlý výzkum chování dětí a mládeže na Internetu. Projektu se zúčastnilo okolo 28 tisíc dětí. Výsledky vyplněných dotazníků byly velmi poučné a staly se zásadním podkladem pro další zvyšování internetové gramotnosti dětí, ale i dospělých. Vyhodnocení potvrdilo to, co odborníci předpokládají: děti se nezdráhají prozradit jakékoliv osobní či intimní informace osobám, které „znají“ pouze z on-line prostředí.

Oba velikáni, Seznam a Google, se snaží prostřednictvím svých projektů „Seznam se bezpečně“ a „Centrum pro bezpečnost Google“ naučit mladé uživatele Internetu osvojit si základy jeho bezpečného používání a tím maximálně snižovat případná rizika. Jejich informace a rady jsou neméně cenné pro samotné rodiče. Pokud ohrožené dítě či dospívající má zábrany a obává se se svým problémem, zejména z oblasti kyberšikany svěřit rodičům, nebo pedagogovi, může požádat o pomoc přímo na těchto portálech.

S dostupností počítačů se na Internetu rozšířila aktivita další ohrožené skupiny, seniorů. Podle Českého statistického úřadu se rok od roku jejich počet zvyšuje, jen v roce 2017 se jednalo o 660 tisíc a to od věkové hranice 65 let výše.[64] Prostřednictvím Internetu z bezpečí domova získávají přehled o dění ve světě, komunikují, zapojují se v diskuzních fórech, vzdělávají se on-line, nakupují. Jejich koníčkem vesměs bývá nevědomé šíření hoax. Nástrahy však číhají v podobě podvodných inzerátů a reklam cílených na jejich věkovou kategorii, kdy následně přicházejí o úspory. Skrytou hrozbou je i mylný pocit anonymity, který je příčinou vyzrazení důvěrných osobních informací.

V České republice na poli osvěty působí mnoho neziskových, nebo multizdrojově financovaných organizací, které mnohdy spolupracují s obdobnými organizacemi na mezinárodní úrovni. Své služby poskytují státní správě, školám i široké veřejnosti, jejich programy jsou určeny pro všechny věkové kategorie. Formou konferencí, školení, přednášek, seminářů a kurzů cílí na bezpečné užívání informačních a komunikačních technologií, bezpečný pohyb na Internetu včetně rizik sociálních sítí a prevenci kybernetické kriminality. Již několik let působí celorepublikový certifikovaný *Projekt E-bezpečí* (www.e-bezpeci.cz), který je realizován Centrem prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého ve spolupráci s dalšími organizacemi a současně podporován Ministerstvem vnitra ČR, Ministerstvem školství,

[64] ČESKÝ STATISTICKÝ ÚŘAD. *Na internetu přibývá seniorů.* [online]. 27.03.2018 [cit. 2019-05-25] Dostupné z WWW: <https://www.czso.cz/csu/czso/na-internetu-pribyva-senioru>

mládeže a tělovýchovy a Policií ČR.[65] Dalším významným projektem určeným pro širokou veřejnost je *bezpečný internet.cz* (www.bezpecnyinternet.cz) založený Českou spořitelnou a společnostmi Microsoft a Seznam.cz.

Řetěz bývá silný jako jeho nejslabší článek, v tomto kontextu je takto vnímán koncový uživatel, který aplikuje prvky zabezpečení. Stejný uživatel svou činností, vyhledáváním služeb nebo ukládáním dat a informací je určitou autoritou, která zásadně ovlivňuje pohyb v kyberprostoru.

[65] Projekt E-Bezpečí. *O projektu*. [online] © 2008-2018 [cit. 2019-05-28] Dostupné z WWW: <https://www.e-bezpeci.cz/index.php/o-projektu/oprojektu>

Závěr

Kybernetická kriminalita, jejíž vývoj je přímo úměrný rozvoji informačních a komunikačních technologií, se řadí k fenoménům současnosti. Předmětem bakalářské práce bylo v dostatečné míře, i když s omezenou kapacitou, shrnout zásadní dílčí aspekty v této oblasti.

V rámci naplnění cíle jsou po úvodní kapitole definovány bezprostředně související základní pojmy a osvětleno obecné působení práva v kyberprostoru. Následně jsou nastíněny prvopočátky a historický vývoj této kriminální činnosti.

Třetí kapitola tvoří co do rozsahu podstatnou část. Jsou zde specifikovány kybernetické hrozby, charakteristika pachatelů, používané nástroje k této trestné činnosti a samotné kybernetické útoky, kdy počítač je jednak využit jako prostředek k jejich spáchání, jednak se stává terčem těchto útoků. Z uvedeného vyplývá, že kybernetická kriminalita se neustále vyvíjí a dílem inteligence, vynalézavosti a nadstandardního technického vybavení pachatelů zaznamenává i širokou variabilitu a vysokou sofistikovanost.

Čtvrtá kapitola se věnuje problematice odhalování a vyšetřování, z čehož je patrné, že obor kybernetické kriminality vyžaduje specifickou metodiku. K tomuto je zapotřebí nejen kvalitní technické vybavení, ale současně jsou kladeny vysoké nároky na odborné znalosti a neustálé vzdělávání se vyšetřujících expertů. Nabízí se otázka, nakolik jsou v dané oblasti, vyjma vyšetřovacích týmů, orgány činné v trestním řízení fundované, zejména z řad soudců.

Pátá kapitola analyzuje právní předpisy. Nastiňuje vývoj legislativy na mezinárodní a vnitrostátní úrovni jak z oblasti trestněprávního postihu, tak z oblasti kybernetické bezpečnosti. Pozornost je zejména věnována významné Evropské úmluvě o počítačové kriminalitě, jež mimo jiné zavázala signatáře k implementaci daných požadavků do vnitrostátních zákonů. Česká republika reagovala přijetím nového Trestního zákoníku, který tak zahrnuje dotčené skutkové podstaty trestných činů kybernetické kriminality. Současná právní úprava rovněž umožňuje zařazení dalších protiprávních jednání z této oblasti i pod mnohé skutky tradičního rázu, z tohoto pohledu se jeví relativně dostačující. Dalším významným legislativním počinem je zákon o kybernetické bezpečnosti ukládající dotčeným subjektům povinnost implementace ochranných mechanismů a spolupráci s národními týmy CERT. V rámci

tohoto je přiblížen proces systému řízení bezpečnosti informací a ochrana soukromí, resp. osobních údajů.

V následující, šesté kapitole, je demonstrováno několik příkladů protiprávních jevů na území České republiky, které jsou současně Policií ČR klasifikovány jako nejfrekventovanější.

Poslední kapitola je zaměřena na prevenci. Jsou popsány metody opatření organizačního a technického rázu vyplývající z aktuální legislativy o kybernetické bezpečnosti, doporučeny možnosti zabezpečení v domácnostech a taktéž podceňovaná ochrana mobilních zařízení. V případě osvěty je třeba zejména klást důraz na dovednosti a on-line chování rizikových skupin k eliminaci ohrožení zdravého vývoje dětí a mládeže a zneužití důvěřivosti z řad seniorů. Gramotnost uživatelů ICT by měla být řazena ke všeobecnému vzdělání a to na všech stupních školství, protože informovanost je jedním z nástrojů, jak předcházet a bránit se rizikům. Ostatně prevence se jeví mnohem účinnější, než-li represe.

Různé celosvětové zdroje se shodují na přibližném počtu uživatelů Internetu, který v roce 2018 dovršil 3,7 miliardy, tedy polovinu populace. Zvyšuje se i počet používaných zařízení, což jde ruku v ruce s rozvojem technologií a tento fakt zákonitě přináší větší požadavky na toky dat nebo úložné kapacity. Na základě těchto skutečností lze očekávat další rozmach kyberkriminality, ať už je motivace útočníků čistě ekonomická, politická či mocenská. Reálný je i předpoklad, že doposud zanalyzované poznatky se stanou zastaralými a na ochranu bude třeba nastavení nových mechanismů. Bezpečnost kyberprostoru a jeho uživatelů bude vyžadovat efektivní zapojení mnoha účastníků a to na všech úrovních, což zahrnuje mezinárodní spolupráci jednotlivých států, policejních organizací s celosvětovým dosahem jako Interpol a Europol, týmů CERT, státního a komerčního sektoru, zejména pak výrobců počítačového vybavení a ochranného software, uživatelů a v neposlední řadě justice. Autoritativní nastavená pravidla by měla umožňovat účinné potírání trestné činnosti v kyberprostoru, současně by však toto prostředí neměla ovládat cenzura. Kybernetická kriminalita je celosvětovou hrozbou a proto boj s ní také vyžaduje globální rozměr.

Seznam použitých zdrojů

Literární zdroje

1. DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat.* Brno: Computer Press, 2004, 190 s., ISBN 80-251-0106-1

2. JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.* [online] Praha : Policejní akademie ČR a Česká pobočka AFCEA, 2015. 240 s. ISBN 978-80-7251-436-6 Dostupné také z WWW: <https://www.afcea.cz/wp-content/uploads/2015/03/Slovnik_v303.pdf>

3. JIROVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha : Grada Publishing, 2007. 284 s. ISBN 978-80-247-1561-2.

4. KALAMÁR, Š., POŽÁR, J. *Vybrané aspekty informační bezpečnosti.* Praha : Policejní akademie ČR, 2010. 190 s. ISBN 978-80-7251-339-0.

5. KOLOUCH, J., VOLEVECKÝ, P. *Trestně právní ochrana před kybernetickou kriminalitou.* Praha : Policejní akademie ČR, 2013. 117 s. ISBN 978-80-7251-402-1.

6. KOLOUCH, J. *Cybercrime.* [online]. Praha : CZ.NIC, 2016. 522 s. ISBN 978-80-88168-18-8. Dostupné také z WWW: <https://knihy.nic.cz/files/edice/cybercrime.pdf>

7. KOLOUCH, J., BAŠTA, P. a kol. *Cybersecurity.* [online]. Praha : CZ.NIC, 2019. 556 s. ISBN 978-80-88168-34-8. Dostupné také z WWW: <https://knihy.nic.cz/files/edice/cybersecurity.pdf>

8. MATEJKA, J. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí.* [online]. Praha : CZ.NIC, 2013. 256 s. ISBN 978-80-904248-7-6. Dostupné také z WWW: <https://knihy.nic.cz/files/edice/internet_jako_objekt_prava.pdf>

9. MATĚJKA, M. *Počítačová kriminalita.* Praha : Computer Press, 2002. 106 s. ISBN 80-7226-419-2.

10. McCARTHY, L. WELDON-SIVIY, D. *Buď pánem svého prostoru.* Praha : CZ.NIC, 2013. 316 s. ISBN 978-80-904248-6-9.

11. PORADA, V., KONRÁD, Z. *Metodika vyšetřování počítačové kriminality.* Praha : Policejní akademie ČR, 1998. 54 s. ISBN 80-85981-75-0.

12. SMEJKAL, V. *Kybernetická kriminalita.* Plzeň : Aleš Čeněk, 2018. 934 s. ISBN 978-80-7380-720-7.

13. ZAVRŠNIK, A. *Kyberkriminalita.* Praha : Wolters Kluwer ČR, 2017. 148 s. ISBN 978-80-7552-758-5.

Elektronické zdroje

1. COUNCIL OF EUROPE PORTAL. *Chart of signatures and ratifications of Treaty 189.* [online]. © 2018 [cit. 2019-05-23] Dostupné z WWW: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=F6wSLE5D>

2. ČESKÁ BANKOVNÍ ASOCIACE. *Češi jsou nepoučitelní, nemění si hesla, nepoužívají mobilní antiviry*. [online]. 22.05.2018 [cit. 2019-05-25] Dostupné z WWW: <https://www.czech-ba.cz/cs/cesi-jsou-nepoucitelni-nemeni-si-hesla-nepouzivaji-mobilni-antiviry>

3. ČESKÁ SPOŘITELNA. *Bezpečnostní desatero*. [online]. Česká spořitelna © 2019 Dostupné z WWW: https://www.csas.cz/cs/o-nas/bezpecnost-ochrana-dat/bezpecnostni-desatero-obecna-pravidla

4. ČESKÝ STATISTICKÝ ÚŘAD. *Na internetu přibývá seniorů.* [online]. 27.03.2018 [cit. 2019-05-25] Dostupné z WWW: <https://www.czso.cz/csu/czso/na-internetu-pribyva-senioru>

5. HOAX.cz. *Infikované jehly na sedadlech.* [online]. Josef Džubák & HOAX.cz. © 2000-2019 [cit. 2019-05-10]. Dostupné z WWW: http://www.hoax.cz/hoax/infikovane-jehly-na-sedadlech/>

6. MINISTERSTVO VNITRA ČR. *Definice pojmu terorismus.* [online]. 29.7.2009 [cit. 2019-02-26] Dostupné z WWW: <https://www.mvcr.cz/clanek/definice-pojmu-terorismus.aspx>

7. MINISTERSTVO VNITRA ČR. *Koncepce boje proti trestné činnosti v oblasti informačních technologií včetně Harmonogramu opatření.* [online]. [cit. 2019-03-15]. Dostupné z WWW: <http://www.mvcr.cz/soubor/koncepce-pdf.aspx>

8. NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. O NÚKIB. [online]. [cit. 2019-04-27] Dostupné z WWW: <https://www.nukib.cz/cs/o-nukib/>

9. OSN. *Všeobecná deklarace lidských práv***.** [online] © 2015 United Nations. [cit. 2019-05-05] Dostupné z WWW: <https://www.osn.cz/wp-content/uploads/UDHR_2016_CZ_web.pdf>

10. POLICIE ČR. *Národní centrála proti organizovanému zločinu. Zpráva o činnosti NCOZ.* [online]. 5.12.2018 [cit. 2019-03-19] Dostupné z WWW: <https://www.policie.cz/vyhodnoceni-cinnosti.aspx>

11. POLICIE ČR. *Nejčastější projevy kybernetické kriminality s odkazem na trestní zákoník.* [online]. © 2019 [cit. 2019-04-27] Dostupné z WWW:<https://www.policie.cz/clanek/nejcastejsi-projevy-kyberneticke-kriminality-s-odkazem-na-trestni-zakonik.aspx>

12. POLICIE ČR. *Kyberkriminalita.* [online]. © 2019 [cit. 2019-05-10] Dostupné z WWW: <https://www.policie.cz/clanek/kyberkriminalita.aspx>

13. POLICIE ČR. *Zpráva o činnosti NCOZ*. [online]. 4. 12. 2018 [cit. 2019-05-10] Dostupné z WWW: <https://www.policie.cz/vyhodnoceni-cinnosti.aspx>

14. PROJEKT E-Bezpečí. *O projektu*. [online]. © 2008-2018 [cit. 2019-05-28] Dostupné z WWW: <https://www.e-bezpeci.cz/index.php/o-projektu/oprojektu>

15. TECHNOR. *ČSN ISO/IEC 27001*. [online]. TECHNOR print, s.r.o. © 2005-2018 [cit. 2019-05-05] Dostupné z WWW: <https www.technicke-normy-csn.cz/369790-csn-iso-iec-27001_4_76533.html>

16. ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Základní příručka k GDPR obecné nařízení.* [online]. © 2013 [cit. 2019-04-27] Dostupné z: https://www.uoou.cz/1-obecne-na-izeni/d-27266

Legislativní dokumenty

1. ČESKO. Zákon č. 89 ze dne 3. února 2012 občanský zákoník. In *Sbírka zákonů České republiky*. 2012, částka 33, s. 1026-1368. Dostupné také z WWW: <https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=89/2012&typeLaw=zakon&what=Cislo_zakona_smlouvy > ISSN 1211-1244.

2. ČESKO. Zákon č. 40 ze dne 8. ledna 2009 trestní zákoník. In *Sbírka zákonů České republiky*. 2009, částka 11, s. 354-464. Dostupné také z WWW: <https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=40/2009&typeLaw=zakon&what=Cislo_zakona_smlouvy > ISSN 1211-1244

3. ČESKO. Sdělení ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě č. 104 ze dne 23. prosince 2013. In *Sbírka sbírka mezinárodních smluv České republiky*. 2013, částka 56, s. 10784-10838. Dostupné také z WWW:

https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=104/2013&typeLaw=mezinarodni_smlouva&what=Cislo_zakona_smlouvy ISSN 1801-0393

4. ČESKO. Zákon č. 412 ze dne 21. září 2005 o ochraně utajovaných informací a o bezpečnostní způsobilosti In *Sbírka zákonů České republiky*. 2005, částka 143, s. 7526-7576. Dostupné také z WWW: <https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=412/2005&typeLaw=zakon&what=Cislo_zakona_smlouvy> ISSN 1211-1244

5. ČESKO. Vyhláška č. 82 ze dne 21. května 2018 o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidace dat (vyhláška o kybernetické bezpečnosti). In *Sbírka zákonů České republiky.* 2018, částka 43, s. 1122-1168. Dostupné také z WWW: <https://www.govcert.cz/download/kii-vis/NovaVKB/VKB_82-2018sb.pdf> . ISSN 1211-1244

Seznam zkratek

BBS	Bulletin Board System *é*
CD	Compact Disc
DNS	Domain Name Systems *systém doménových jmen*
DoS	Denial of Service *odepření přístupu*
DVD	Digital Video Disc *formát digitálního optického datového nosiče*
EFF	Electronic Frontier Foundation *mezinárodní nezisková organizace*
GDPR	General Data Protection Regulation
HDD	Hard Disc Drive *jednotka pevného disku*
HTTP	Hypertext Transfer Protocol
ICT	Informační a komunikační technologie
ICQ	*fonetický přepis* I Seek You, *software pro posílání textových zpráv*
ICMP	Internet Control Message Protocol
IP	Internet Protocol
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Informační technologie
LAN	Local Area Network *lokální počítačová síť*
MMS	Multimedia Messaging Service *multimediální zpráva*
P2P	Per-to-Per
PC	Personal Computer
PIN	Personal Identification Number *osobní identifikační číslo*
PING	Packet Internet Groper
SMS	Short Message Service *krátká textová zpráva*
TCP	Transmission Control Protocol *protokol transportní vrstvy*
WAN	Wide Area Network *rozlehlá počítačová síť*
Wi-Fi	*označení pro bezdrátovou komunikaci*