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

BAKALÁŘSKÁ PRÁCE

KYBERNETICKÁ KRIMINALITA V PROSTŘEDÍ INTERNETU

Autor práce: Lukáš Fojtík

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 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 RNDr. Růženě FEREBAUEROVÉ, za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

FOJTÍK, L. *Kybernetická kriminalita v prostředí internetu : bakalářská práce.* České Budějovice : Vysoká škola evropských a regionálních studií, 2019. 67 s. Vedoucí bakalářské práce : RNDr. Růžena Ferebauerová.

Klíčová slova: počítačová kriminalita, internet, kyberprostor, kyberkriminalita.

Práce analyzuje kybernetickou kriminalitu v prostředí celosvětového systému propojených počítačových sítí – Internetu. Vysvětluje vznik kybernetické kriminality páchané v prostředí internetu od jejího počátku do současnosti. Snaží se analyzovat budoucí možné trendy ve směřování kybernetické kriminality a její použití v návaznosti na nové technické prostředky a vývoj technologií. Práce se také zaměřuje na škodlivé programové kódy, které pachatelé trestné činnosti využívají k útokům na své oběti a které používají jako prostředky ke splnění vytyčených cílů. Dále analyzuje škody napáchané kybernetickými zločinci při použití metody útoku, který se zaměřuje na finanční škody a metody útoku se zaměřením na psychické škody.

ABSTRACT

FOJTÍK, L. *Cybercrime in the Internet Environment : Bachelor Thesis.* České Budějovice : The College of European and Regional Studies, 2019. 67 p. Supervisor : RNDr. Růžena Ferebauerová.

Key words: cybercrime, Internet, cyberspace, cybercriminality.

This thesis analyzes cyber criminality within the worldwide communication network - the Internet. It explains the origin of cyber criminality and its striking development on the Internet up to the present. Moreover, it attempts to analyze probable future trends of cyber criminality, their further applications in connection with new technology devices and technologies. It also describes malicious codes which cause harm to users-victims or are used as means to reach the specific goals of cybercriminals. Furthermore, it assesses the harm caused by cybercriminals when using the method of attack resulting in financial loss, or other methods leading to psychological harm to innocent users.

Obsah

Úvod

Celosvětový systém propojených počítačových sítí neboli síť sítí Internet má od svého počátku stále větší vliv na fungování naší společnosti a stala se fenoménem současnosti. Na této síti je dnes již existencionálně závislá celá naše společnost. Internet nelze nevyužívat, zastavit, smazat či dokonce vypnout, aniž by toto rozhodnutí nemělo dopad na fungování společnosti. Internet každoročně pomáhá řadě státních institucí, firem i běžným uživatelům k zefektivnění jejich práce, při hledání zábavy a informací či k provozování dalších různorodých činností nebo používání služeb, kterými tato síť disponuje. Internet je ve své podstatě neomezenou a stále se rozrůstající sítí, která poskytuje na různých platformách řadu rozličných služeb. V budoucnu lidstvo internet využije ještě různoroději a za pomoci nových technických prostředků. Jeho závislost na internetu bude více prohloubena.

Z prostředí původně provozovaného univerzitami ve Spojených státech amerických se Internet dostal i do běžných technických prostředků (osobních počítačů, mobilů, aut, atd.), které každodenně využíváme. Česká republika byla oficiálně k Internetu připojena 13. února 1992 kdy na ČVUT v Praze byla předvedena funkční zahraniční linka. V roce 2018 mělo zřízeno připojení k internetu už 80% českých domácností. Stále však v počtu připojených domácností Česká republika zaostává za evropským průměrem. V ČR má již přístup k Internetu 7,1 milionu Čechů starších 16 let. V roce 2018 využívalo Internet na svých mobilech 58% Čechů. Použití Internetu se rozšířilo i do mobilních zařízení.[1]

Kvalitní připojení a jeho vysoká dostupnost je předpokladem pro využívání služeb, které uživatelům usnadňují práci a zpestřují volný čas. Stále více lidí se díky dostupnosti Internetu naučilo používat www stránky, sociální sítě, video portály a další služby. Také podíl uživatelů v mobilním bankovnictví rok od roku prudce roste. Aktivní klient se do mobilního bankovnictví přihlásí i několikrát týdně. Lidé začínají k nákupům využívat internetové obchody. U některých komodit již tyto obchody nahradily kamenné prodejny.

Počítače v dnešní době vlastní velká většina českých domácností (78%) a mobilní telefon už vlastní skoro každý občan ČR (96%). Internet se stal nedílnou

[1] *Podíl domácností s internetem stoupl na 80 %, ČR zaostává za EU* [online]. Praha : ČTK, 2019 [cit. 2018-11-23]. Dostupné z WWW: <https://www.ceskenoviny.cz/zpravy/podil-domacnosti-s-internetem-stoupl-na-80-cr-zaostava-za-eu/1688960>.

součástí každodenního života a pomocníkem pro uživatele, vlády, státní organizace, ozbrojené složky a soukromé firmy.[2]

Prostředí Internetu bohužel skrývá i své temné stránky. V hlubinách Internetu se pohybují lidé, kteří se snaží zůstat před očima běžných uživatelů, orgánů činných v trestním řízení (OČTŘ), vládními organizacemi i médii skryti. Tito lidé v prostředí Internetu páchají rozličnou trestnou činnost. Používají jej jako přenosové prostředí ke splnění svých cílů ať již k zisku finančních prostředků, nebo cíleného útoku na vybranou osobu, stát, kritickou infrastrukturu nebo jiné subjekty. V prostředí Internetu se kriminalitě velmi dobře daří. Tato kriminalita je odborníky nazývaná kybernetickou kriminalitou (angl. Cybercrime).

Kyberkriminalita se zrodila v okamžiku, kdy osobní počítače zdomácněly a staly se dostupné velkému počtu obyvatel. A také v okamžiku, kdy uživatelé tyto počítače začali k Internetu připojovat. Dalšímu rozšíření dopomohlo mobilní internetové připojení. Možnost oprostit se od toho, být připoután na jedno fyzické místo, je pro pachatele lákavou variantou. Do budoucna po vzniku automatizovaných systémů, které bude pohánět umělá inteligence a které budou sloužit státním institucím, policii nebo armádě k potlačování kyberkriminality, bude mobilita pro pachatele nutností. V blízké budoucnosti se pachatelé ještě více zaměří na chytré mobilní telefony. Některé k útokům využijí, na jiné budou útoky zaměřeny.

Pachatelem trestné činnosti v oblasti kybernetické kriminality dnes už nemusí být jenom crackeři, ale mnohdy to jsou cizí státy, teroristé, organizované skupiny zločinců nebo sami uživatelé. Od „soukromých“ hackerů a útokům na finance se pachatelé trestné činnosti v Internetu přesunuli k „státním“ hackerům a útokům na kritickou infrastrukturu státu a/nebo k ideologickým a propagačním útokům, šířením dezinformací, informační válce apod. Z kybernetické kriminality se vyčlenila i její podmnožina – kybernetický terorismus.

Většina provedených trestných činů je dnes páchána v kyberprostoru. Internet pachatelům kybernetické kriminality slouží jako přenosové prostředí, do kterého jsou připojeni jejich oběti. V kyberprostoru mohou při velmi nízkých nákladech zaútočit na veškerá spojení, dopravu, energetické systémy, bankovnictví, průmysl nebo obranné

[2] *Podíl domácností s internetem stoupl na 80 %, ČR zaostává za EU* [online]. Praha : ČTK, 2019 [cit. 2018-11-23]. Dostupné z WWW: <https://www.ceskenoviny.cz/zpravy/podil-domacnosti-s-internetem-stoupl-na-80-cr-zaostava-za-eu/1688960>.

prostředky státu. Svým jednáním tak mohou způsobit velmi velké škody při minimálním úsilí a nákladech. Tyto útoky jsou citelnější a „bolestnější“ pro technologicky vyspělejší země nebo technologicky závislejší uživatele. Celkové vnímání Internetu uživateli i útočníky se od jejího prvního nasazení radikálně změnilo.

1 Cíl a metodika bakalářské práce

Bakalářská práce je rozdělena na několik částí: popisnou, teoretickou a závěrečnou část. Ve všech částech práce bude postupováno na základě stanovených cílů a metodiky.

V první části je záměrem autora zaměřit se na vymezení základních pojmů souvisejících s kybernetickou kriminalitou a dále popis jejích jednotlivých forem současně s jejím vznikem a historií. První část je založena především na studiu oborné literatury a odborných článků, které o kybernetické kriminalitě pojednávají.

Prostředí Internetu je velice různorodé, stejně jako kriminalita páchaná v tomto prostředí. Její formy, vznik a historie jsou velmi obsáhlým tématem. Záměrem autora bakalářské práce je především přehledně uvést jednotlivé formy počítačové kriminality vyskytující se v prostředí Internetu. Autor se v první části nejprve věnuje vymezení nejširších základních pojmů v oblasti kyberprostoru, které slouží k pochopení rámce práce. Poté jsou popsány základní pojmy kybernetické kriminality páchané v prostředí Internetu. První část také zahrnuje historii kybernetické kriminality se zaměřením na její možný budoucí vývoj spolu s trendy, kterými se kyberkriminalita může v budoucnu ubírat.

Cílem první části je přehledně shrnout základní pojmy kybernetické kriminality, její historii a budoucí vývoj spolu s poukázáním na její nejpoužívanější formy.

Teoretická část bakalářské práce je založena na analýze kybernetické kriminality v prostředí Internetu a na jejím průběhu. V druhé části je rozbor případu kybernetické kriminality, který byl zaměřen na finanční škody s celosvětovým dopadem. Dále pak rozbor případu kybernetické kriminality, zaměřeného na psychické škody i s jejími dalšími důsledky, které jsou spojené s psychickou újmou.

Cílem teoretické části bakalářské práce je provedení analýz popsaných případů kybernetické kriminality, které se zaměřily na napáchání finančních a psychických škod. Dále byl na konci teoretické části shrnut fakt, jak se nárůst počítačové kriminality promítnul do současné společnosti se zhodnocením vývoje bezpečnosti v České republice.

Závěrečná část práce obsahuje stručné shrnutí a zhodnocení výsledků obou předchozích částí práce. V závěrečné části bakalářské práce jsou také popsány možné budoucí trendy využití technického pokroku kyberzločinci. V této části je kladen důraz na prevenci a obranu proti útokům. Vzhledem k obsáhlosti a prolnutí témat počítačové kriminality páchané v prostředí Internetu a jejích příčin nebylo možné striktně oddělit popisnou část od části teoretické. Snahou autora práce je, aby toto prolnutí bylo srozumitelné a dalo ucelený pohled na počítačovou kriminalitu.

2 Vymezení základních pojmů

Používání internetového prostředí přináší uživatelům mnohé výhody, ale také velká rizika. Každý počítač připojený k Internetu je potencionálním terčem pachatelů trestné činnosti (útočníků) nebo terčem škodlivých počítačových kódů. Nepoučený uživatel je však přesvědčen o své vlastní anonymitě a anonymitě své činnosti při surfování na vlnách Internetu. Domnívá se, že jemu se nic z toho, co se v prostředí Internetu děje přece nemůže stát. Toto přesvědčení je velmi nebezpečné a nezakládá se na pravdě. Každý uživatel Internetu se jednou stane obětí útočníka. Neznalost a nezájem o toto téma ze strany uživatelů jen zvětšuje šance pachatele k úspěšnému provedení útoku.

Z historického pohledu se pro osoby, které se snaží neoprávněně dostat do osobních počítačů jiných uživatelů proti jejich vůli a skrytě vžil termín „hacker“. Tento termín bohužel nevystihuje podstatu tohoto anglického slova ani člověka, který se za ním skrývá. Slovem hacker je v médiích i mezi laickou veřejností označován člověk, který se snaží neoprávněně proniknout do jejich osobního počítače, počítačové sítě, kritické infrastruktury nebo systému. Pro potřeby práce není toto slovo v práci v kontextu kybernetické kriminality využíváno a autor upřednostnil použití slova útočník, nebo přesného označení – cracker.[3]

V současné době počítače ve větší míře pronikají do každodenního života naší společnosti a již nelze nalézt lidskou činnost, kde by se výpočetní technika přímo, nebo zprostředkovaně nepoužívala. S vyššími nároky na použití výpočetní techniky roste četnost jejího zneužívání k různorodé trestné činnosti.

Některé pojmy nejsou v ICT (Information and Communication Technologies – Informační a komunikační technologie) do mateřských jazyků překládány. Ani mezi odborníky nepanuje jednoznačná shoda ve vymezení těchto pojmů a v předkladu slov a to i z důvodu jejich občasné nejednotnosti a rozdílného chápání obsahového významu. Pro potřeby práce jsou tyto pojmy a slova přeloženy, doplněny o český ekvivalent, nebo ponechány v původním znění, pokud by překlad byl matoucí. V dalších kapitolách jsou vymezeny základní pojmy, které jsou potřebné pro pochopení kontextu práce a následujících kapitol.

[3] *Cracker* [online]. San Francisco (CA) : Wikimedia Foundation, 2001 [cit. 2018-11-04]. Dostupné z WWW: <https://cs.wikipedia.org/wiki/Cracker>.

2.1 Cyberspace

Termín Cyberspace (kyberprostor) použil jako první americký spisovatel William Gibson na počátku 80. let ve své povídce Jak vypálit Chrome (angl. Burning Chrome). V pozdější povídce Neuromancer popsal Cyberspace jako „sdílenou halucinaci“.[4] Až v dalších letech se začaly objevovat přesnější a odbornější definice tohoto pojmu. Kyberprostor nemá hmotnou podstatu, je imaginární, nehmotný. Přesto je jeho existence přímo závislá na reálném světě. Je chápán jako nehmotný svět informací, který vzniká vzájemným propojením informačních a komunikačních systémů. Podle zákona o kybernetické bezpečnosti a o změně souvisejících zákonů se v § 2 písm. a) kybernetickým prostorem rozumí digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.[5] Kyberprostor představuje klíčový prvek v definici kybernetické kriminality a je pevně spjat s prostředím internetu. Kyberprostorem je někdy internet mylně označován, ale toto označení není zcela přesné. Kyberprostor internet ve své definici přesahuje. „Světové počátky Internetu, který je nezbytnou materiální podstatou kyberprostoru, se datují do 50. let 20. století. V té době došlo k budování a testování sítí propojených počítačů především pro vědeckovýzkumné a vojenské účely. Ačkoli byl Internet vybudován na základech sítí ARPANET a NSFNET, v současné době není nikdo vlastníkem Internetu a neexistuje ani centrální autorita či instituce, která by jej řídila.“[6]

2.1.1 Underground kyberprostoru

Kyberprostor není sestaven pouze z viditelné části označované anglicky jako Surface Web. Jsou v něm obsaženy i neviditelné části označované Dark Web a Deep Web. Definice neviditelných webů (Dark Web, Deep Web) nejsou mezi odborníky jednotné. Dalšími názvy neviditelné části kyberprostoru mohou být Hidden Web, Invisible Web, Darknet atd. Deep a Dark weby jsou také někdy označovány jako D4rkN3ts (Darknets).

Viditelný web (angl. Surface Web) je tou částí v kyberprostoru, která je běžnému uživateli nejznámější. Zahrnuje indexované a uživatelsky běžně dostupné webové stránky. Kybernetický prostor si lze představit jako pomyslný ledovec, kde

[4] *Cyberspace* [online]. Sharpened Productions, 2019 [cit. 2018-11-04]. Dostupné z WWW: <https://techterms.com/definition/cyberspace>.
[5] ČESKO. Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In Sbírka zákonů, Česká republika. 2014, částka 75, s. 1926-1936.
[6] KOLOUCH, J. *Cybercrime*. Praha, 2016, s. 42.

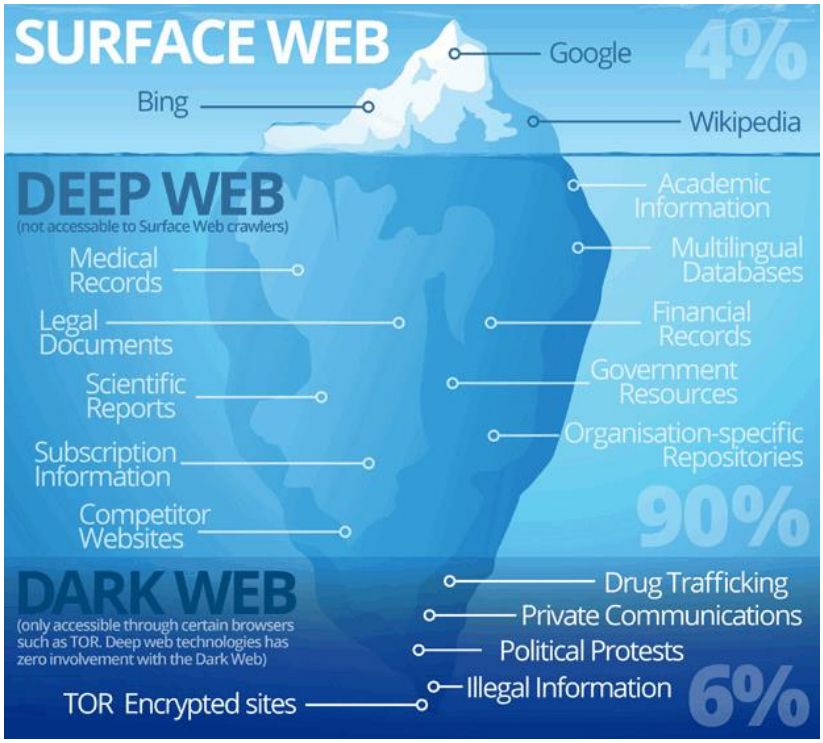
běžný uživatel se pohybuje pouze ve viditelné části. O ostatních částech většina z nich nemá ani pojetí. Kyberprostor je pro běžného uživatele jen internet a ještě jen pouze jedna viditelná část – Surface Web.[7]

Deep Web není pro uživatele běžně dostupný. Nelze jej najít v indexovaném vyhledávání. Odhadem obsahuje více než 90% informací, které se dají na kyberprostoru nalézt. Deep Web obsahuje akademické informace, lékařské záznamy, vědecké zprávy, finanční záznamy a jiné. Pro náhodného uživatele je většina těchto informací nedostupná a zabezpečená. Přístup k některým z nich je řízen na základě uživatelských oprávnění a je vyžadována příslušnost k dané skupině (např. pracovník výzkumu) nebo pozvánka.

Dark Web je část Deep Webu přístupná pouze díky speciálním prohlížečům jako je například Tor. Tyto prohlížeče zaručují uživatelům naprostou anonymitu při přístupu k Darknetu. Tyto sítě nejsou na snadno dohledatelné a pro přístup je potřeba výše zmíněného klienta Tor. „Tor je založen na přeposílání komunikace přes síť serverů zapojených do systému, kde internetové adresy odesílatele a příjemce nejsou čitelné v žádném kroku cesty. Příjemce zná pouze adresu posledního zprostředkujícího stroje a není možné určit, kdo s kým komunikuje.“[8] Jedná se o skryté domény (sítě), které nesou příponu .onion. Tento název byl zvolen na základě podobnosti s cibulí, kdy uživatel přistupující k této doméně se díky klientovi dostává po vrstvách do stále větších hlubin kyberprostoru (Internetu). V prostředí Dark Webu jsou k nalezení i Dark Markets. Jedná se o tržiště, kde probíhají různé typy obchodů (legálních i nelegálních). Dark Markets nabízejí obchod s kryptoměnami, drogami, zbraněmi, nelegálním software a dalšími komoditami. Poskytují také služby ve formě nájemného crackingu, spamové kampaně, útoku ransomware apod.[9] Uživatelé v prostředí Darknets mohou najít řadu ilegálních informací, politických manifestů, návodů na výbušné zařízení atd.

[7]KOLOUCH, J. *Cybercrime.* Praha, 2016, s. 46-47.
[8] SMEJKAL, V. *Kybernetická kriminalita.* Plzeň, 2018, s. 81.
[9] SMEJKAL, V. *Kybernetická kriminalita*. Plzeň, 2018, s. 82.

Obrázek 1: Rozdělení Kyberprostoru[10]



2.1.2 Internet

Slovo internet pochází z latinské předpony inter (česky mezi) a anglického slova net (network – síť). Původně to bylo označení pouze jedné ze sítí, ale postupem času došlo k zobecnění názvu. Nejmarkantnější službou poskytovanou prostřednictvím Internetu je WWW (kombinace textu, grafiky a multimédií propojených v jedné zobrazované stránce). Najdeme však zde i další poskytované služby jako jsou internetová televize, rozhlasové stanice, emailové služby, obchody, a mnoho jiných.

Internet je největší celosvětová počítačová síť, ve které mezi sebou počítače komunikují pomocí protokolu TCP/IP.[11] Počet zapojených počítačů do Internetu se každým dnem skokově zvyšuje. Internetem jsou vzájemně propojeny všechny kontinenty, státy i jednotlivé počítače v domácnostech. V poslední době je stále zřetelnější propojení „starého“ Internetu, kde byly spolu propojeny pouze počítače s Internetem „novým“, který se skládá z mobilních telefonních sítí. Do těchto sítí jsou zapojeny mobilní telefony a v budoucnu sem budou zapojeny také další věci (např. auta,

[10] *Dark Web – The Unexplored Cyberspace* [online]. San Francisco (CA) : Medium.com, 2018 [cit. 2019-02-22]. Dostupné z WWW: <https://medium.com/coinmonks/dark-web-the-unexplored-cyberspace-5009ca0ecd87>.
[11] JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti* [online]. Praha, 2013, s. 49.

ledničky, pračky). Internet věcí (Internet of Things) bude jednou z dalších evolucí Internetu. Už dnes umožňuje připojení k Internetu řada elektronických zařízení: počítač, mobil, tablet, televize, herní konzole, ledničky a další. Veškeré činnosti prováděné těmito zařízeními spočívají v získávání, přenosu, ukládání, zpracování a šíření dat. Všechny tyto připojené věci jsou pro útočníky potencionálními přístupovými body, obzvláště pak pokud jsou ponechány bez aktualizací a oprav.

Materiální hmotnou podstatou Internetu je jeho páteřní síť, která vede signál (data) vzduchem, kabely, či jinými přenosovými médii. Technicky se jedná o celosvětovou distribuovanou počítačovou síť složenou z jednotlivých menších sítí, které jsou navzájem spojeny jedinou sjednocující technologií. Tím je umožněna komunikace, přenos dat, informací a poskytování služeb mezi subjekty navzájem.[12]

2.1.3 Cloud computing a webová úložiště

Webová úložiště (Google Disk, Microsoft One-Drive, RapidShare, Ulož.to, iCloud, atd.) díky napojení na Internet slouží uživatelům k ukládání různých dat, která pak mohou pohodlně uživatelé sdílet mezi sebou. Webová úložiště nabízejí takzvaný zjednodušený cloud computing.

Cloud computing je způsob používání informačních technologií a služeb, které pro uživatele vzdáleně zprostředkovává server umístěný v Internetu. Uživatel má na svém osobním počítači nainstalovaného klienta (aplikaci), který umožňuje spojení a komunikaci mezi PC a vzdáleným serverem (úložištěm). Veškerý výpočetní výkon pro zabezpečení požadované služby je počítán na straně serveru. Toto řešení přináší řadu výhod, ale i nevýhody. Mezi nevýhody patří vzdáleně uložená data, která mohou být pro potencionální útočníky lákavou a snadnou kořistí, obzvláště pokud provozovatel zanedbá údržbu nebo počítačovou bezpečnost. Útočníkovi přináší cloud computing výhodu ve formě velkého výpočetního výkonu při vtvoření botnetu, kterému bude cloud computing propůjčovat výpočetní výkon a strojový čas.[13]

Blízká budoucnost ICT je v cloud computingu, na který v již dnes přechází řada soukromých společností a státních institucí.

[12] KOLOUCH, J. *Cybercrime*. Praha, 2016, s. 43.
[13] SMEJKAL, V. *Kybernetická kriminalita*. Plzeň, 2018, s. 59-64.

2.1.4 Hacker

Hacker je „osoba: (1) která se zabývá studiem a prozkoumáváním detailů programovatelných systémů nejčastěji pro intelektuální zvídavost a tuto schopnost si neustále zdokonaluje (White hat), (2) kterou baví programování a která dobře a rychle programuje, (3) která je expertem pro určitý operační systém nebo program, například UNIX. Pojem Hacker se často nesprávně používá pro osoby, které zneužívají svých znalostí při pronikání do informačního systému a tak porušují zákon.“[14]

S pojmem Hacker se pojí i další pojmy:

- „Hackers for hire (H4H) akronym pro hackery, kteří nabízejí své služby jiným kriminálním, teroristickým nebo extremistickým skupinám (najmutí hackeři)“ [15] za úplatu.

- Hactivism je použití hackerských dovedností a technik k dosažení politických cílů a podpoře politické ideologie. Hactivism vznikl ze slov hack a activism. Nejznámější hactivistickou skupinou jsou Anonymous. Skupina má ve svém znaku masku Guye Fawkese. [16] A způsobila již celou řadu neoprávněných průniků do cizích systémů a jiné kybernetické zločiny.

- White hat je „etický hacker, který je často zaměstnáván jako expert počítačové bezpečnosti, programátor nebo správce sítí. Specializuje se na penetrační testy a jiné metodiky k zajištění IT bezpečnosti v organizaci.“[17]

2.1.5 Cracker

Slovo Cracker vzniklo z anglického výrazu „safe cracker“. Toto slovo označuje pachatele, který se pokouší prolomit kód sejfu a proniknout k jeho obsahu. Cracker ve světě ICT je osoba, která se pokouší získat neoprávněný přístup k počítačovému systému. Crackeři mají k dispozici prostředky k prolamování se do systémů a pro uživatele jsou velmi nebezpeční. Mohou se dělit na Black Hat, Bot herder a Password Cracker. Bot herder je „cracker, který ovládá velké množství

[14]JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti* [online]. Praha, 2013, s. 40.
[15]JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti* [online]. Praha, 2013, s. 41.
[16] JIRÁSEK, P., NOVÁK, L, POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti* [online]. Praha, 2013, s. 41.
[17]. JIRÁSEK, P., NOVÁK, L, POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti* [online]. Praha, 2013, s. 111.

zkompromitovaných strojů (robotů, botů, zombií)“ nebo „nejvyšší počítač v hierarchii botnetu ovládající zkompromitované počítače daného botnetu“ [18] (sítě s infikovanými počítači). Black hat je skupina crackerů, kteří vytvářejí a následně pak rozesílají počítačové viry a červy. Pomocí nich se pak snaží neoprávněně proniknout do cizího systému za účelem krádeže dat, nebo vyřazení části či celé sítě z provozu. Password cracker je osoba zaměřená na prolamování hesel.

2.2 Kybernetická trestná činnost

Kybernetická trestná činnost je charakterizována jako páchání trestné činnosti, v níž hraje důležitou roli počítač, větší množství počítačů, chytré zařízení (mobilní telefon) nebo jiná komponenta s určitým výpočetním výkonem. Kybernetická kriminalita je tedy trestná činnost, která se v daném čase odehrává v kyberprostoru (Internetu).

Kybernetická kriminalita se transformovala z počítačové kriminality. Toto například definuje Smejkal ve své knize Počítačové právo. Pod pojmem počítačová kriminalita je tedy třeba chápat páchání trestné činnosti, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení včetně dat, nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď:

a) jako předmět této trestné činnosti, ovšem s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité,

b) jako nástroj trestné činnosti.[19]

“Namísto pojmu počítač je v dnešní době používán spíše výraz informační a komunikační technologie (Information and Communication Technology -ICT), resp. Trestné činy v ICT.“[20] Z uvedeného je jasně patrné, že v minulosti byla počítačová kriminalita chápána odlišně, než ji chápeme v současnosti. Dnes může útočník k útoku použít chytrý mobilní telefon nebo jiný sofistikovaný prostředek, který v porovnání se starými počítači má stejný, ale spíše vyšší výpočetní výkon.

[18]. JIRÁSEK, P., NOVÁK, L, POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti* [online]. Praha, 2013, s. 25.
[19] SMEJKAL, V., VLČEK, M., SOKOL, T. *Počítačové právo*. Praha, 1995, s. 99.
[20] KOLOUCH, J. *Cybercrime*. Praha, 2016, s. 32.

Pro spoustu pachatelů jsou morální aspekty trestného činu páchaného v kyberprostoru snáze snesitelné, než morální aspekty krádeže ve fyzickém světě. Manipulace s daty je pro pachatele v řadě případů rychlejší, než manipulace s tištěnými dokumenty. Vymazání nebo úprava dat je mnohem snazší v kybernetickém prostoru a pachatel po sobě zanechá jen velmi málo stop. Kontrola zanechaných stop ve výpočetní technice je mnohem složitější, než kontrola stop při vloupání do obchodu. Trestné činy páchané v kybernetickém prostředí mají velmi velkou úspěšnost a velmi slabou míru odhalení (vysokou míru latence). Při páchání kyberkriminality ICT odborníkem navíc úspešnost a pravděpodobnost neodhalení narůstá.

Pod kybernetickou trestnou činnost se řadí mnoho druhů činností, které mají za cíl napáchat škody, vyřadit systém z provozu nebo zaútočit na data uživatelů. Nejsou ojedinělé ani finanční machinace. Dělení kybernetické trestné činnosti je vnímáno odborníky odlišně. Práce se zaměřuje na nejvíce využívané pojmy kybernetické kriminality.

3 Historie kybernetické kriminality

Kybernetická kriminalita kopíruje technologický pokrok a možnosti jednotlivých technických prostředků. „Rámcové rozhodnutí Rady EU č. 2002/584/JHA o evropském zatýkacím rozkazu označuje za computer-related crime takové jednání, které směřuje proti počítači, či jednání, kde je počítač prostředkem ke spáchání trestného činu.“[21] Znění tohoto rozkazu může sloužit jako jedna z definic kybernetické kriminality. Výkladový slovník kybernetické bezpečnosti (Cyber Security Glossary) ve svém druhém aktualizovaném vydání definuje kybernetickou kriminalitu (Cyber Crime) takto: „Trestná činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení (včetně dat), nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět zájmu této trestné činnosti (s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité) nebo jako prostředí (objekt) nebo jako nástroj trestné činnosti.“[22] Z uvedených definic kybernetické kriminality je patrné, že rámcově vymezit tuto kriminalitu je velmi obtížné. Různé

[21]KOLOUCH, J. *Cybercrime*. Praha, 2016, s. 33.
[22]JIRÁSEK, P., NOVÁK, L, POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti* [online]. Praha, 2013, s. 41.

právní normy vnímají kybernetickou kriminalitu rozdílně a stejně tak ji rozdílně mohou vnímat jednotliví odborníci, organizace, média, orgány činné v trestním řízení a soudy.

Možné klasifikace kybernetické kriminality dle Koloucha z knihy Cybercrime:

- „Klasifikace dle Úmluvy o kybernetické kriminalitě a dle dodatkového protokolu;
- Klasifikace Commitee of Experts on Crime in Cyberspace;
- Klasifikace dle eEurope+;
- Klasifikace počítačové trestné činnosti dle kriminalistiky;
- Zaměření Europolu na některé druhy kybernetické kriminality dle závažnosti;
- Další možné klasifikace kyberkriminality (dle četnosti útoků, postižitelnosti právem dle míry tolerance většinovou společností).“[23]

3.1 První trestné činy páchané v kyberprostoru

Historicky prvními trestnými činy páchanými v kybernetickém prostoru byly sabotáže. Ty prováděli zaměstnanci s cílem poškodit zaměstnavatele, nebo různí aktivisté s cílem vyjádřit nesouhlas s politikou. Úplně první počítačová sabotáž byla provedena v 19. století na tkalcovském stroji, který byl řízen děrnými štítky v manufaktuře pana Josefa Jacquarda, vynálezce tkalcovského stroje na děrné štítky.[24]

Při stále narůstajícímu počtu kriminálních činů páchaných na počítačích začali orgány pověřené kontrolou a prevencí počítačové kriminality uvažovat o jejich sběru a vyhodnocování. V USA zajišťoval sběr údajů o zneužití počítačů již od roku 1958 Stanford Research Institute. Údaje byly rozděleny do několika kategorií, mezi nimi byl například vandalismus, krádež majetku, krádež počítačového času apod. Zprvu nebyla zaznamenávána data nijak relevantní. V roce 1968 bylo zaznamenáno pouhých 13 případů. V roce 1977 už ale institut zaznamenal 85 případů. Jeden příklad za všechny hovoří o obvinění viceprezidenta brokerské firmy, který neoprávněně děroval speciální datové štítky. Díky nim si na svůj soukromý účet převedl v průběhu 8 let 250 tisíc

[23]KOLOUCH, J. *Cybercrime*. Praha, 2016, s. 57-58 .
[24]YONAZI, J. J., SEDOYEKA, E., ARIWA, E., EL-QAWASMEH, E. *e-Technologies and Networks for Development.* Heidelberg, 2011, s. 172.

dolarů. Institut sbíral data až do roku 1978, kdy byl projekt ukončen.[25] V české republice se o sběr údajů stará Policie ČR od roku 2011.[26]

První počítačový zločin se v ČR datuje do sedmdesátých let minulého století, kdy nespokojený zaměstnanec poškodil magnetem záznamy na magnetických páskách, čímž vyřazoval počítač LEO 326 z provozu. Tím hrubě porušil pracovní morálku a zároveň způsobil zaměstnavateli ztrátu dat. Tento člověk byl podle neověřených informací odsouzen za sabotáž na více než 10 let.[27] Podobný případ se objevil později, když pracovníci výpočetního střediska záměrně poškozovali počítač sovětské výroby (SMEP), z důvodu špatného překladu interpretačního programovacího jazyka (tehdejší operační systém) a jeho velké poruchovosti. Pachatelé chtěli tímto způsobem dosáhnout výměny za kvalitnější počítač vyrobený v západní Evropě, nebo USA.[28]

Při příchodu sofistikovanějších počítačů a počítačových systémů se na nové technologie začali adaptovat i pachatelé. Na vzestupu bylo falšování údajů v běžných pracovních dokumentech. Byly to například různé manipulace se mzdovými podklady, zásobovacími podklady a jinými dokumenty zpracovávanými na počítačích. Později s narůstající počítačovou gramotností si pachatelé začali uvědomovat, že mnohem snazší a jednodušší je měnit údaje přímo na počítači, než k těmto změnám počítač využívat. Tento krok, ale znamenal, že pachatel musel mít udělený plný přístup k počítači, což v minulosti nebylo zrovna jednoduché. Dalšími z mnoha trestných činů minulosti bylo i využívání veškerých dostupných prostředků počítače k osobnímu využití, nebo k vlastnímu obohacení. Toto jednání by se dalo charakterizovat jako neoprávněné užívání cizí věci.[29]

Distanční trestná činnost byla v minulosti zcela bezpředmětná, jelikož počítače spolu nebyly propojeny žádnými sítěmi. Internet byl teprve vznikající pojem. V technologicky zaostalých zemích východního bloku o něm vědělo jen několik málo lidí. Díky nízkému počtu počítačů, slabé znalosti jejich obsluhy mezi laickou veřejností a vztahem občanů ke společnému socialistickému vlastnictví je pro tuto dobu zároveň typická vysoká míra latence počítačových deliktů. Toto všechno bylo umocněno pocity,

[25]MUSIL, S. *Počítačová kriminalita*. *Nástin problematiky*. Praha, 2000, s. 23.
[26]*Kyberkriminalita* [online]. Praha : Policie ČR, 2019 [cit. 2019-02-22]. Dostupné z WWW: <www.policie.cz/clanek/kyberkriminalita.aspx>.
[27]SMEJKAL, V. *Kybernetická kriminalita*. Plzeň, 2018, s. 105.
[28] FIALOVÁ, R. *Počítačová kriminalita v České republice* [online]. Brno : Masarykova univerzita, 2001 [cit. 2018-12-05]. Dostupné z WWW: <ttps://www.fi.muni.cz/usr/jkucera/pv109/2001/xfialov1.html>.
[29]SMEJKAL, V. *Kybernetická kriminalita*. Plzeň, 2018, s. 102.

že počítačový (strojový čas) má zvláštní charakter nehmotného majetku. Výpočetní čas přece nelze ukrást. V souvislosti se sálovými počítači už neexistovala žádná další trestná činnost než ta, která byla uvedena výše.[30]

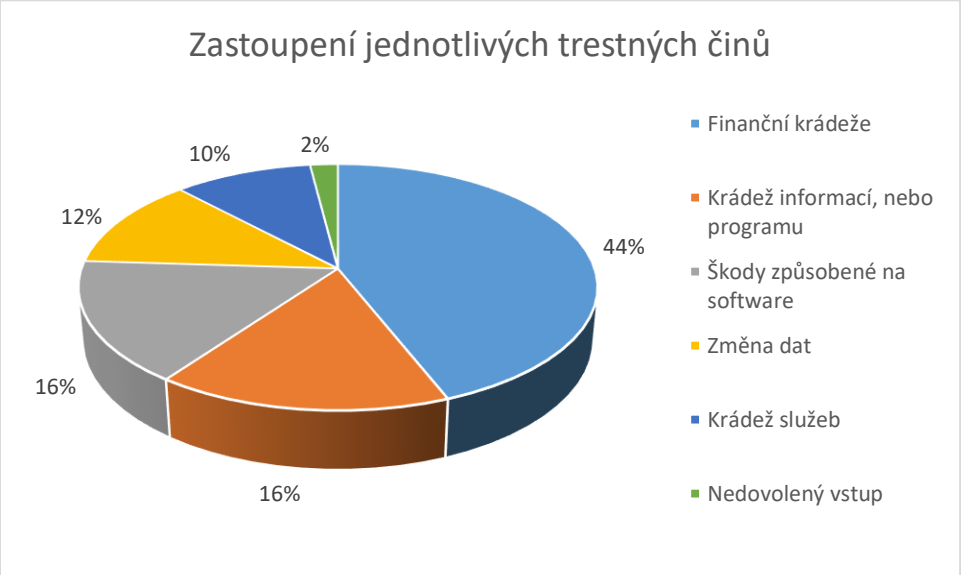
3.2 Osmdesátá a devadesátá léta

V 80. letech byly hlavními tématy kybernetické kriminality krádeže databází, šíření virů, infiltrace logických a časových bomb přímo do operačních systémů a rozšiřování a využívání nelegálního programového vybavení. Velké publicity se dostalo zvlášť jednomu ze zločinů, který byl podrobně popsán v knize Cliffa Stolla Kukaččí vejce. Jde o autentický příběh autora a astronoma pana Stolla. Ten v Lawrence Berkley Laboratory 10 měsíců pracoval na monitorování probíhajících průniků do různých počítačů náhodně zjištěného crackera, kterého sám Stoll pojmenoval Willy Hacker. Willy Hacker se pokusil o přístup do celkem 450 počítačů, které provozovala americká armáda nebo její dodavatelé. Z tohoto počtu bylo celkem 30 pokusů úspěšných. Z Williho Hackera se později vyklubal západoněmecký specialista s údajným propojením na KGB. Na jeho sledování se musely podílet a spolupracovat americké i německé úřady a jiné soukromé organizace.[31]

V devadesátých letech se na poli kybernetické kriminality staly velké změny. Počítače začaly být v západních zemích dostupné pro širší masy a firmy i státní instituce je začínaly zapojovat do svého portfolia k usnadnění práce. V těchto letech se začíná celosvětově rozšiřovat Internet. Dochází k jeho prvnímu zneužití k šíření pornografie, rasismu a dalšího závadného obsahu. Díky Internetu se také začínají jednotliví pachatelé slučovat do organizovaných skupin. Pozadu v používání Internetu při prosazování svých vlastních cílů nezůstávají ani zpravodajské služby, média či extrémisté. V USA byly jednotlivé trestné činy na poli kybernetické kriminality zastoupeny takto: [32]

[30]SMEJKAL, V. *Kybernetická kriminalita*. Plzeň, 2018, s. 179-180.
[31]MUSIL, S. *Počítačová kriminalita*. *Nástin problematiky*. Praha, 2000, s.23 – 24.
[32]MUSIL, S. *Počítačová kriminalita*. *Nástin problematiky*. Praha, 2000, s. 24.

Graf 1: Zastoupení jednotlivých kybernetických trestných činů v USA[33]



V ČR bylo v devadesátých letech páchání kybernetické kriminality spíše ojedinělým činem. To bylo způsobeno díky malému zastoupení osobních počítačů a nízké úspěšnosti OČTŘ při jejich odhalování. Většina osobních počítačů navíc nebyla připojena k Internetu. Jeden příklad za všechny: „V roce 1998 u *Městského soudu* byla obžalovaná dvojice pachatelek, 24letá dcera a její matka, z podvodného vybírání celkové sumy 9 700 000 Kč. Do počítačového systému vstoupila a podvod spáchala jedna z pachatelek, v době činu úřednice *Komerční banky* tak, že se vydávala pomocí odpozorovaného hesla a fingovaných podpisů za svoji kolegyni, autorizovanou uživatelku systému.“[34]

3.3 Nástup nových technologií

Nástup nových technologií a samotný technologický pokrok, který umožnil hromadné využívání počítačů, stál za vznikem neméně masivního nárůstu počítačové kriminality. Podle Smejkala v knize Kybernetická kriminalita se „nová doba kybernetické kriminality datuje dvěma zásadními momenty:

- „nástupem osobních počítačů,
- vznikem počítačových sítí a vzdáleného přístupu k počítačům,

K těmto dvěma faktorům musíme připojit ještě třetí, a to:

[33]MUSIL, S. *Počítačová kriminalita*. *Nástin problematiky*. Praha, 2000, s. 24.
[34]MUSIL, S. *Počítačová kriminalita*. *Nástin problematiky*. Praha, 2000, s. 24.

- exponenciální růst možností mobilní telefonie a tomu odpovídající vybavenost občanů, včetně využívání anonymních, tzv. předplacených karet.“[35]

Autor práce s názory pana Smejkala souhlasí. Nové technologie vytvořily živnou půdu pro pachatele, kteří je začali využívat ke splnění svých vlastních cílů. Odtud už je pro pachatele vše mnohem snáze proveditelnější. Klasické podvody byly vylepšeny a začaly se objevovat jejich nové formy, jako je například pharming a phishing. Typově se pachatelé začali měnit. Stejně tak se začaly měnit základní charakteristiky trestné činnosti, kterou pachatelé prováděli.

Díky propojení počítačů do sítí a později do Internetu se zaměření pachatelů obrátilo proti uživatelům Internetu a distanční trestná činnost začala nabírat na obrátkách. Se stále větším nárůstem počtu počítačů, které do Internetu byly připojovány, úměrně narůstal i počet pachatelů, kteří v jeho prostředí prováděli trestnou činnost. Internet dokonce pachatelům umožňoval a do současné doby umožňuje značně potlačit hranice jednotlivých států a kontinentů. Pachatelé jsou díky Internetu schopni svou oběť napadnout z úplně opačného konce planety. V závislosti na Internetu a propojení velkého množství počítačů se staly poměrně populární i velmi jednoduché typy útoků, avšak s plošnými následky. Útoky typu DoS, DDoS, nasazování podvodných emailů, falešných zpráv, ransomware, spyware a další, jsou jednoduchou formou útoku. U těchto typů útoků nemusí být pachatel ICT odborníkem.

Další vývoj vedl ke vzniku „vládních“ hackerských skupin a jejich mnohačetných útoků na kritické infrastruktury postižených států. Neobvyklá není ani průmyslová špionáž nebo krádeže technologií. Také teroristické skupiny nezahálely a začaly vytvářet vlastní hackerské složky. Kyberterorismus a kybernetická válka se od počítačové kriminality vyčlenily a staly se samostatným odvětvím.

[35]SMEJKAL, V. *Kybernetická kriminalita*. Plzeň, 2018, s. 103.

4 Kybernetická kriminalita v prostředí Internetu

Prostředí Internetu je specifické a unikátní. Je mylné předpokládat, že i zde budou platit stejná pravidla a vzorce chování, jako v reálném světě. Každoročně ve světě stoupá počet zařízení a uživatelů, kteří se k Internetu připojují, viz obrázek 2.

Obrázek 2: Světová populace a užití Internetu[36]

WORLD INTERNET USAGE AND POPULATION STATISTICS						
JUNE 30, 2018 - Update						
World Regions	Population	Population	Internet Users	Penetration	Growth	Internet
	(2018 Est.)	% of World	30 June 2018	Rate (% Pop.)	2000-2018	Users %
Africa	1,287,914,329	16.9 %	464,923,169	36.1 %	10,20%	11.0 %
Asia	4,207,588,157	55.1 %	2,062,197,366	49.0 %	1,70%	49.0 %
Europe	827,650,849	10.8 %	705,064,923	85.2 %	570%	16.8 %
Latin America / Caribbean	652,047,996	8.5 %	438,248,446	67.2 %	2,33%	10.4 %
Middle East	254,438,981	3.3 %	164,037,259	64.5 %	4,89%	3.9 %
North America	363,844,662	4.8 %	345,660,847	95.0 %	219%	8.2 %
Oceania / Australia	41,273,454	0.6 %	28,439,277	68.9 %	273%	0.7 %
WORLD TOTAL	7,634,758,428	100.0 %	4,208,571,287	55.1 %	1,07%	100.0 %

Mezi hlavní znaky Internetu patří jeho snadná dostupnost, otevřenost, interaktivita, globálnost, decentralizovanost a informační bohatost. V takovém prostředí je pro pachatelé snadné zůstat anonymní a skrýt se před zraky vyšetřovatelů.

Internet svým uživatelům přináší mnohem lepší dostupnost služeb z pohodlí domova nebo mobilního telefonu. Uživatel připojený k Internetu může dnes z domova nakoupit jídlo, automobil, přečíst si novinky ze zahraničí i z domova, diskutovat k určitým tématům v rámci odborných i laických fór a v neposlední řadě posílat různé formy dat.[37] Toto je jenom krátký výčet veškerých možností Internetu, který samozřejmě nabízí mnohem více služeb, některé na hraně nebo za hranou zákona. V Internetu můžeme nalézt informace k výrobě výbušného zařízení, témata podněcující k rasové nesnášenlivosti, pornografii všeho typu, autorsky chráněné programy, knihy, filmy atd. Internet přinesl společnosti informační revoluci a sám o sobě je velmi silné informační médium. Díky výše popsanému jsou možnosti, které mají pachatelé trestné činnosti takřka neomezené a poměrně široké. Chápání Internetu se mezi jeho uživateli změnilo a stále se vyvíjí.

[36]*INTERNET USAGE STATISTICS. The Internet Big Picture* [online]. Bhópál : Miniwatts Marketing Group, 2018 [cit. 2018-12-30]. Dostupné z WWW: <www.internetworldstats.com/stats.htm>.
[37]*Internet* [online]. San Francisco (CA) : Wikimedia Foundation, 2001 [cit. 2018-12-14]. Dostupné z WWW: <https://wikipedia.org/wiki/Internet>.

Kybernetická kriminalita v období po připojení počítačů k Internetu zažila nebývalý rozmach. Objevují se zde nové skutkové podstaty trestných činů. Nové druhy důkazů i velká množina nových právních problémů. Kybernetická kriminalita je odborníky považována za nový druh kriminality, i když velkou většinu současně známých a dobře popsaných projevů trestné činnosti přenáší do kybernetického prostředí. V tomto prostředí je pro pachatele její provedení mnohem jednodušší, rychlejší a efektnější než v prostředí fyzickém. V prostředí Internetu ale začaly vznikat i nové trestné činy, které se ve fyzickém světě nevyskytují. Jsou to například hacking, DoS a DDoS útok, botnet a další. Prostředí Internetu má svá vlastní pravidla a vzorce lidského chování oproti prostředí reálnému a lidé se zde nechovají stejně jako v reálném světě. Jeden příklad za všechny: člověk, který by v obchodě nikdy neukradl DVD s autorským obsahem (film, hudba, atd.), stahuje na Internetu autorsky chráněná díla bez skrupulí. Navíc je dále distribuuje mezi své přátele a známé či dokonce prodává. Podobných nepochopitelných vzorců chování lze při páchání kybernetické kriminality mezi lidmi nalézt celou řadu. Kybernetická kriminalita představuje celosvětový problém.

V dalších podkapitolách jsou popsány nejpoužívanější typy hrozeb, které mohou „číhat“ na neznalého uživatele při surfování na vlnách Internetu.

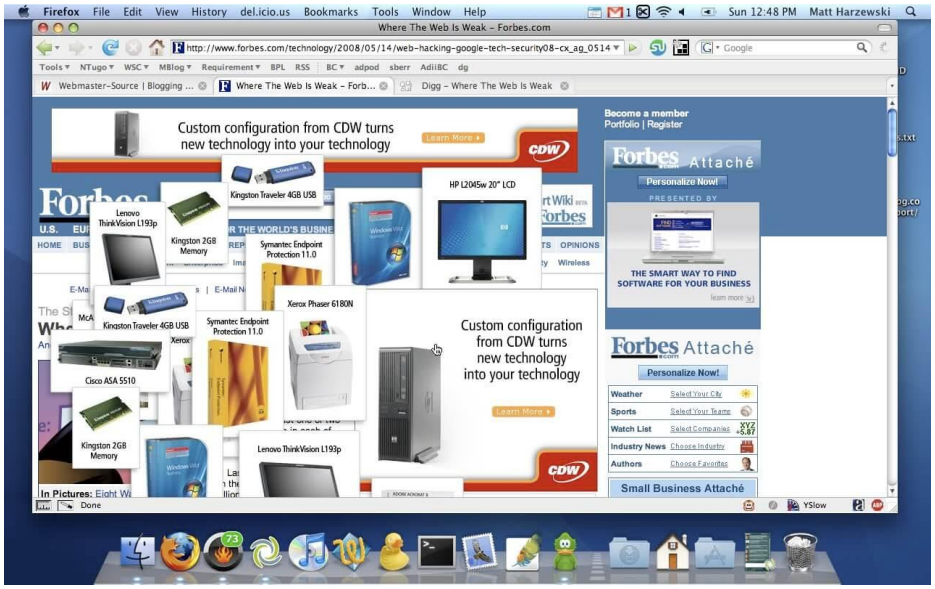
4.1 Malware

Zde je vhodné zmínit základní škodlivé programy, které mohou pachatelé využívat a pomocí nich dosáhnout svého cíle. Některé programy jsou sofistikovanější, jiné zase obtížně odhalitelné nebo kombinace obojího. Malware (malicious software - nežádoucí software) je uživatelem nevyžádaný program, který je pro cílový technický prostředek (počítač, tablet, mobil, atd.) škodlivý a který byl do technického prostředku instalován bez vědomí a souhlasu uživatele. Malware je velká množina pojmů. Každý autor může ke skupině malware přistoupit odlišně. Dělení malware může být následující:

Adware (advertising supported software) – nevyžádaná reklama všeho druhu. Tento software často bývá současně distribuován ve freewarových nebo sharewarových programech. Projevy adware mohou být mírné – reklamní banner ve spodní části používaného programu nebo velmi nepříjemné – vyskakovací pop-up okna. Jedná se o nevyžádanou reklamu, která postiženého uživatele obtěžuje a nedovoluje mu pohodlně pracovat. Pachatelé mohou díky adware rozesílat reklamy s klikacími

návnadami (clickbait). Popis titulku nebo reklamní obrázek, který odkazuje na stránku s adware je vytvořen tak, aby byl pro uživatele lákavý ke kliknutí. Po kliknutí se uživatel přesune na stránku s malwarem a ten se mu nainstaluje do PC.[38]

Obrázek 3: Adware[39]



Backdoor (zadní vrátka) jsou programy, které na technickém prostředku vytvářejí průchody, které útočník využije k nepozorovanému proniknutí do počítačového systému. Backdoory jsou podobné trojským koním.

Keylogger (sledování stisku kláves) tento typ malware sleduje jednotlivé stisky kláves a údaje o jejich používání pak odesílá útočníkovi. Zaměření tohoto programu je zejména v odchycení přihlašovacího jména a hesla.[40]

Ransomware (požadavek na výkupné) je v poslední době velice populární typ malwaru, který zašifruje data na pevném disku. Jejich dešifrování je zpoplatněno a útočník následně data (možná) dešifruje. Tento typ malwaru bude podrobněji popsán v kapitole 6. kybernetická kriminalita zaměřená na finanční škody.[41]

[38]KOLOUCH, J. *Cybercrime*. Praha, 2016, s.205.
[39]*Adware: Definition and Removal Guide* [online]. Copenhagen : hemdalsecurity.com, 2017 [cit. 2019-01-13]. Dostupné z WWW: < https://heimdalsecurity.com/blog/adware-definition-removal>.
[40]*What is a Keylogger?* [online]. Moskva : Kaspersky, 2019 [cit. 2019-01-13]. Dostupné z WWW: <https://www.kaspersky.com/resource-center/definitions/keylogger>.
[41]*What is Ransomware?* [online]. Moskva : Kaspersky, 2019 [cit. 2019-01-13]. Dostupné z WWW: <https://www.kaspersky.com/resource-center/definitions/what-is-ransomware>.

Obrázek 4: Ransomware[42]

Rootkit – do této oblasti spadají počítačové programy i celé technologie, které pomáhají zamaskovat přítomnost malware na technickém prostředku uživatele. Jsou hojně využívány k zamaskování virových nákaz nebo sledovacího softwaru.

Scareware jsou falešné programy, které mezi uživateli záměrně způsobující paniku. Jedná se například o program, který provede falešnou kontrolu počítače. Vystraší uživatele tím, že nahlásí nespočet problémů, které je potřeba urychleně odstranit. Jejich odstranění je samozřejmě zpoplatněno.[43]

[42] *Easy, Cheap, and Costly: Ransomware is Growing Exponentially* [online]. San Jose (CA) : umbrella.cisco.com, 2015 [cit. 2019-01-13]. Dostupné z WWW: <https://umbrella.cisco.com/blog/2015/09/02/easy-cheap-and-costly-ransomware-is-growing-exponentially>.

[43] *What is a Scareware?* [online]. Moskva : Kaspersky, 2019 [cit. 2019-01-13]. Dostupné z WWW: <https://www.kaspersky.com/resource-center/definitions/scareware>.

Obrázek 5: Scareware[44]

Spyware (složenina z anglických slov spy - špion a software) jsou sledovací programy, které se snaží získat různé údaje, nebo vypozorovat uživatelovy návyky. Skrytě pak útočníkovi odesílají získané informace na předem naprogramovanou adresu. Mohou také vysledovat přístupová hesla a jména. Spyware může obsahovat i další skryté nástroje, ovlivňující uživatelský komfort a bezpečnost technického prostředku.[45]

Trojan horse (trojský kůň) je program, který se vydává za jiný program. Obsahuje nezveřejněné funkce, se kterými uživatel nesouhlasil a není s nimi obeznámen. Bez vědomí uživatele pak skrytě na jeho technickém prostředku provádí nevyžádanou činnost, naplánovanou útočníkem.

Virus – nežádoucí škodlivý program, který je schopen samostatného šíření a infikování jednotlivých počítačů i mimo síť většinou pomocí USB flash disku, formou spustitelného souboru typu EXE, dokumentu nebo obrázku. V minulosti byly viry nejrozšířenější formou infikování počítače útočníkem. Jejich použití bylo od zobrazení různých výzev, spouštění nevyžádané hudby až po úplné zablokování počítače a ztrátu dat. Viry se dokáží samy šířit a také infikovat další počítače připojené v síti. V dnešní

[44]*The ultimate guide to scareware protection* [online]. New York : ZDNet, 2009 [cit. 2019-01-13]. Dostupné z WWW: < https://www.zdnet.com/article/the-ultimate-guide-to-scareware-protection/>.
[45]*What is a Spyware? - Definition* [online]. Moskva : Kaspersky, 2019 [cit. 2019-01-13]. Dostupné z WWW: < https://www.kaspersky.com/resource-center/threats/spyware>.

době se spíše viry snaží chovat skrytě. Mohou bez vědomí uživatele odesílat data, jeho zvyky, ale i instalovat další nežádoucí SW.[46]

Obrázek 6: Varování před PC virem[47]

Worm (červ) – červi nepotřebují ke svému šíření žádný spustitelný soubor a jsou úzce spjati s viry. Šíří se samostatně a převážně v prostředí síťové infrastruktury. Pro počítačovou síť jsou velmi nebezpeční, protože dokážou vysledovat mezery v jejím zabezpečení a také ji dokáží vyřadit z provozu.[48]

4.1.1 Šíření malware v prostředí Internetu

Existuje celá řada sofistikovaných distribucí škodlivého programového vybavení. Jeho šíření může být přes DVD, CD, USB Flash Disky, emailové zprávy, kancelářskými soubory typu DOC, EXE, XLS, a jinými. Malware může být přítomen i v HTML kódu webových stránek. Níže je popsán nejnebezpečnější typ distribuce malware v prostředí Internetu a tou je forma drive-by-download. Kolouch ve své knize Cybercrime popisuje drive-by-download takto: „Drive-by-download - jeden

[46] *What is a Computer Virus or a Computer Worm?* [online]. Moskva : Kaspersky, 2019 [cit. 2019-01-13]. Dostupné z WWW: < https://www.kaspersky.com/resource-center/threats/viruses-worms>.
[47] *Antivirové kukátko: dnes Avast!* [online]. Praha : Zive.cz, 2005 [cit. 2019-01-13]. Dostupné z WWW: <https://www.zive.cz/clanky/antivirove-kukatko-dnes-avast/sc-3-a-122212/default.aspx>.
[48] *What is a Computer Virus or a Computer Worm?* [online]. Moskva : Kaspersky, 2019 [cit. 2019-01-13]. Dostupné z WWW: < https://www.kaspersky.com/resource-center/threats/viruses-worms>.

z nejčastějších způsobů infikování technického prostředku pomocí malware je jeho stažení z Internetu a následně pak spuštění infikovaného souboru s příponou .EXE z neznámého zdroje.“[49]

Drive-by-download je běžná technika používaná útočníky ke skrytému nainstalování malwaru na technický prostředek oběti. Útočník infikuje běžnou webovou stránku škodlivým kódem a čeká, nebo láká svou oběť například prostřednictvím emailu nebo sociálních sítí k jejímu navštívení. Útočník ale může infikovat i webovou stránku, o které si již předtím zjistil, že ji oběť často navštěvuje. Oběti se stránka jeví normálně a nelze poznat jakoukoli změnu provedenou útočníkem. Na počítači oběti při návštěvě stránky probíhá (většinou na pozadí) skrytá instalace malwaru. Útočník umně využije známých zranitelností a svých technických znalostí k úpravě, nebo napsání Java pluginu. Plugin provede vzdálené připojení ke stanici pachatele a stažení několika instancí jiných škodlivých kódů. Tyto kódy plugin následně spustí (mohou to být trojské koně, spyware, keylogger atd.). Podle svých vlastností tyto kódy provedou napsané instrukce. Některé z nich útočníkovi umožní užití vzdáleného přístupu k technickému prostředku oběti. Jiné pro útočníka shromažďují informace o oběti (hesla, navštívené stránky apod.) a odesílají je pak na útočníkovo vzdálené úložiště. Útočník získá díky těmto pomocníkům o své oběti důležitá data, hesla k přístupu k osobnímu, nebo firemnímu emailu, hesla do firemní sítě, čísla bankovních účtů a jiná zajímavá data. Tyto data pak může využít ke svému obohacení, nebo vydírání oběti.[50]

Detekce takovýchto útoků je závislá na kombinaci mnoha faktorů a je velmi obtížná. Velká většina případů není odhalena, některé případy jsou odhaleny až po několika týdnech či měsících od napadení. Skupina malware programů je rozsáhlá a v prostředí Internetu hojně rozšířená.

„Malware je možné nainstalovat téměř do jakéhokoli počítačového systému.“[51] V roce 2017 a v roce 2018 byl na vzestupu malware typu ransomware, který dominoval všem zveřejněným statistikám. Malware už nedistribuují pouze počítačoví „nadšenci“ v současné době to jsou profesionálové, kteří se na své činnosti snaží vydělat a stále častěji jsou zapojeni do organizovaných skupin.

[49]KOLOUCH, J. *Cybercrime*. Praha, 2016, s. 211-213.
[50]*Drive-by Downloads* [online]. Australia : Australian Government, 2012 [cit. 2018-12-01]. Dostupné z WWW: <https://acsc.gov.au/publications/protect/Drive-by-Downloads.pdf>.
[51]KOLOUCH, J. *Cybercrime*. Praha, 2016, s. 217.

4.1.2 Sociální inženýrství

Předpokladem pro provedení úspěšného kybernetického útoku je podle autora práce precizně naplánované sociální inženýrství. Jedná se o „způsob manipulace lidí za účelem provedení určité akce nebo získání určité informace. Ve většině případů útočník nepřichází do osobního kontaktu s obětí. Útoky obsahují prvky přesvědčování a manipulace. Jsou vedeny buď náhodně, nebo cíleně na konkrétní osoby. Sociální inženýři se dokáží poučit ze svých chyb. Svoje útoky dokáží neustále vylepšovat a přizpůsobovat prostředí.“[52]

Klíčovým faktorem při provádění sociálního inženýrství je vytěžení co nejvíce informací, co nejpečlivější sběr dat a jejich vyhodnocení. K tomu aby došlo k tak obrovskému sběru dat a informací o oběti, musí být útočník s obětí v kontaktu mnohdy několik dní a musí s ní navázat důvěrný vztah. Útočník musí mít dobré znalosti lidského chování a psychiky a být odborníkem v manipulaci. Sociální inženýrství je stále zdokonalováno a útoky začínají být propracovanější a kvalitnější. Útoky jsou vedeny kombinací sběru dat o oběti s formami psychického a fyzického útoku za cílem zisku požadovaných informací. Tento typ útoku je mnohem nebezpečnější, než by se na první pohled mohlo zdát. Sociální inženýrství je hojně využívaným typem útoku na sociálních sítích. Zde slouží k navázání důvěry mezi pachatelem a jeho obětí. Nejčastějšími obětmi jsou zde děti, které na sociální síti postují veškeré informace o sobě bez zábran. Z tohoto důvodu by rodiče měli mít dohled nad dětmi a jejich činnostmi v prostředí Internetu. Útočníci ale nemusejí své oběti oslovovat přímo přes sociální sítě, mohou k tomu použít veřejné chaty, fóra a jiné diskuze.

4.2 Boty a botnety

Bot nebo taky zombie computer je počítač, který byl útočníkem záměrně a skrytě infikován. Tento počítač čeká na útočníkův povel k provedení naplánované akce. Mezitím se připojí k centrálnímu řídícímu serveru (command-and-control server) spolu s ostatními takto infikovanými boty. Útočník (botmaster), který má kontrolu nad celou sítí (botnet) si tak vytváří superpočítač s možností centralizované správy a velkým výpočetním výkonem.

„Botnety je možné využít k řadě činností, avšak v popředí je především finanční zisk, který spočívá jak v generování vlastních útoků (např. ransomware, phishing,

[52]KOŽÍŠEK, M., PÍSECKÝ V. *Bezpečně na internetu. Průvodce chováním ve světě online*. Praha, 2016, s. 37.

rozesílání spamu, krádežím informací, DDoS aj.), tak v pronájmu svých služeb či celého botnetu klientům. Díky výše popsanému je možné botnet zařadit do struktury crime-as-a-service (kde je nabízena služba: botnet-as-a-service), či do malware economy, kde představuje základní technickou platformu, nezbytnou pro provedení celé řady kybernetických útoků.“[53]

4.3 Kybernetická kriminalita jako služba

V ICT je dnes v popředí všeho zájmu kromě cloudových služeb i budování informačních systémů ve formě služby (princip xxxx-as-a-service) ať už ve spojení s cloudovým řešením nebo bez něj. Z tohoto důvodu existuje i v undergroundu Kyberprostoru nabídka kybernetického zločinu jako služby (cybercrime-as-a-service). Pachatelé zde poskytují své znalosti a dovednosti. Za jejich použití očekávají stanovený profit. Kdokoliv se tak může zapojit do páchání trestné činnosti v prostředí Internetu v rámci služby Crime-as-a-service.

Mezi nabízené služby patří odhalování zranitelností člověka, cílového počítačového systému, softwaru nebo specifické síťové infrastruktury. Úprava malware dle zadání objednatele. Pronájem počítačové sítě k využití výpočetního výkonu. Objednávka na prolomení hesel. Vedení sofistikovaných a cílených útoků a dokonce lze jako službu objednat i spamovou kampaň. V rámci pořekadla fantazii se meze nekladou je možné na těchto marketech jako službu objednat téměř jakýkoliv zamýšlený druh kybernetické kriminality, kterou pak lze v kyberprostoru využít. V budoucnosti bude tento druh trestné činnosti nabývat na významu.

4.4 Scam

Spam je hromadné šíření nevyžádané elektronické pošty v prostředí Internetu nejčastěji typu reklamního sdělení nebo jiných poštovních zpráv (phishing), které mohou mít navíc v přílohách škodlivý kód. Šíření malware za pomocí spamové kampaně, odborně nazýváme Scam (švindl). Při využití sociálního inženýrství se Scam snaží přesvědčit uživatele o nutnosti kliknutí na podvrženou stránku nebo otevření závadné přílohy. Mezi scam patří:

- Phishing „v českém překladu je možné vyložit tento termín jako „rybaření“. Jde o podvodnou techniku, která je založena na získávání údajů, jimiž mohou být hesla, kreditní karty nebo jiné údaje. Většinou je metoda

[53] KOLOUCH, J. *Cybercrime*. Praha, 2016, s. 196.

Phishingu využívána v elektronické komunikaci, kde se pod nějakou záminkou (e-maily ze služby, banky, sociální sítě), snaží získat z uživatelů citlivé údaje.“[54] Phishing je pro pachatele hojně používaným nástrojem.

- Malware viz kapitola 4.1.

- Nigerijské dopisy – druh kybernetické kriminality byl přenesen z reálného prostředí. Jedná se o dopisy, které informují uživatele o velké výhře, potřebě někomu finančně pomoci či o dědické příležitosti. Velkou měrou jsou psány špatnou gramatikou. Na první pohled je u některých dopisů jasné, že jsou do češtiny strojově přeloženy. Podvodníci se snaží z oběti primárně vylákat finanční částku. V poslední době zaznamenáváme stále více se lepšící překlady do mateřského jazyka. Toto je způsobeno tím, že útočníkům pomáhají čeští občané, nebo že tyto útoky sami páchají.

- Podvodné loterie a nabídky – elektronickou poštou na Internetu šířené podvodné nabídky a loterie k nalákání na neexistující předměty, které jsou inzerovány k prodeji. Pachatelé požadují od své oběti platbu předem, ale k předání zboží nedojde. Jedná se o velmi často používanou formu trestné činnosti, podvodné nabídky se běžně schovávají na bazarových portálech mezi nabídkami skutečnými. Na první pohled je nelze od skutečné nabídky řádně rozeznat.

- Hoax (kachna) poplašná zpráva na Internetu, kterou si mezi sebou posílají uživatelé (tím ji řetězí) a která často obsahuje prosby o pomoc, varování před nějakou činností, výzvy, petice, prohlášení apod.

4.5 Nebezpečí číhající na Internetu

Trestných činů páchaných v prostředí Internetu může být celá řada. Europol každoročně sumarizuje uplynulý rok na poli kybernetického zločinu v dokumentu IOCTA (Internet Organised Crime Threat Assessment), který se zaobírá hodnocením hrozby organizovaného zločinu v prostředí Internetu.[55] Na pomyslném vrcholu škodlivých programů používaných kybernetickými zločinci již několik let zpětně je malware typu ransomware. Roste počet nových typů malwaru, které se zaměřují na těžbu virtuálních

[54]KOŽÍŠEK, M., PÍSECKÝ V. *Bezpečně na internetu. Průvodce chováním ve světě online*. Praha, 2016, s. 123.
[55]EUROPOL. *IOCTA: Internet Organised Crime Threat Assessment* [online]. Europol : European Cybercrime Centre, 2018 [cit. 2019-01-20]. Dostupné z WWW: <www.europol.europa.eu>.

finančních prostředků (kryptoměn). Stále častější je instalace škodlivého programového kódu za využití známých slabin operačních systémů a programů.

Bohužel hrozbou je rostoucí počet případů, kdy jsou pachateli kyberkriminality obtěžovány děti. Hranice věku dětí pro přístup k Internetu a sociálním sítím se snížila. Pro dnešní děti je přístup do sítě Internet mnohem snazší. Rozšířeným se stává i placený live streaming sexuálního zneužívání dětí.

Pachatelé nezaostávají ani ve finančních podvodech, podvodech za použití falešných Internetových obchodů a nabídka v obchodech s kybernetickou kriminalitou (Darknet Marketplace) se také rozšířila. Přibývají i další jazykové mutace těchto obchodů. Neutuchají ani „Nigerijské dopisy“, nebo spamové kampaně.

Prostředí Internetu je velmi rozličné a různorodé. Kybernetická kriminalita v tomto prostředí nezahrnuje pouze výše vyjmenovaných několik nejznámějších druhů. Každý druh kybernetické kriminality může mít svůj poddruh. Mezi další hojně využívané prostředky v Internetu jsou: Internetové pirátství, sniffing, DoS, DDoS, DRDoS útoky, šíření závadného obsahu atd. Díky větší vzdělanosti pachatelů, kteří ke svým útokům využívají nabídky různých anonymizačních a šifrovacích nástrojů je pro orgány činné v trestním řízení stále obtížnější tyto pachatele na Internetu najít a jejich činnost odhalit. V ČR bylo v roce 2016 spácháno přes 5600 trestných činů v oblasti kybernetické kriminality. Více než polovina byly majetkové trestné činy. Je mylné se domnívat, že se kyberzločinci zaměřují převážně na firmy a obyčejného uživatele se tento problém netýká.[56] Bezpečí uživatelů Internetu je tedy v jejich vlastních rukou a snaze dozvědět se o technologiích, jejich fungování a možných hrozbách, plynoucích z jejich používání co nejvíce informací. Paní Catherine De Bolle, výkonná ředitelka Europolu ve výroční zprávě IOCTA prohlásila: “Pouze když policejní sbory, soukromý sektor a akademická sféra budou úzce spolupracovat, můžeme s kybernetickým zločinem bojovat efektivně.“[57]

[56]RÁŽ, J. Interview. *Fokus Václava Moravce* ČT24. TV, ČT24, 12. prosince 2017, 59:00.
[57]EUROPOL. *IOCTA: Internet Organised Crime Threat Assessment* [online]. Europol : European Cybercrime Centre, 2018 [cit. 2019-01-20]. Dostupné z WWW: <www.europol.europa.eu>.

5 Vývoj kybernetické kriminality na Internetu

Bruce Schneier mezinárodně uznávaný bezpečnostní expert o vývoji kybernetické kriminality na Internetu v roce 2002 na své stránce v podsekci jménem Crypto-Gram prohlásil, že zločinci mají tendenci zaostávat za vývojem technologií o pět až deset let, ale nakonec si uvědomí její možnosti. Stejně jako když Willie Sutton vykrádal banky, protože „tam jsou peníze“, tak i zločinci začnou útočit na počítačové sítě, protože stále více hodnot se ukládá online, než do trezorů. Pokoutně změnit číslo v bankovní databázi je mnohem bezpečnější, než napochodovat do banky se zbraní v ruce.[58]

5.1 Nové směry kybernetické kriminality

Kyberzločinci neustále hledají nové směry a cesty páchání trestné činnosti. Nejnovější trendy kybernetické kriminality směřují na chytré telefony – univerzální zařízení, kterému lidé svěřují citlivé osobní informace a které je propojeno s bankovními účty, sociálními sítěmi i jinými zařízeními a službami. Mobilní telefon s operačním systémem se stal součástí technické vybavenosti občana. Je používán v takové míře, že přístup k Internetu přes mobilní zařízení z velké míry začíná přebírat vedoucí postavení na úkor přístupu z PC. Uživatelé by měli pochopit, že v kapse nenosí pouze mobilní telefon. V kapse nosí plnohodnotný počítač, který o nich shromažďuje data a na který se dá zaútočit úplně stejně, jako na stolní počítač.[59]

S rozvojem mobilních telefonů a sítí vznikne nové hřiště pro vedení kybernetických útoků. Rozšíření mobilních sítí 5. generace a zavedení Internetu věcí (IoT – Internet of Things) se dotkne každého z nás. V roce 2019 rezonuje kauza společnosti Huawei (Čínská polostátní společnost, zaměřující se na mobilní technologie), kdy některé tajné služby tvrdí, že výrobky společnosti skýtají pro uživatele blíže neupřesněná bezpečnostní rizika.[60] Při zavedení IoT a připojení různých věcí k Internetu budou mít pachatelé ještě více ucelený přehled o chování svých obětí. Informace získané z těchto věcí využijí k provedení útoku, sociálnímu inženýrství nebo ke spáchání trestné činnosti.

[58]*Crypto-Gram: Crime:The Internet's Next Big Thing* [online]. New York : Schneier Security, 2002 [cit. 2019-01-21]. Dostupné z WWW: <https://www.schneier.com/crypto-gram/archives/2002/1215.html>.
[59]RÁŽ, J. Interview. *Focus Václava Moravce* ČT24. TV, ČT24, 12. prosince 2016, 1:04:00
[60]NOVÁK, M., Chripák, D. *Grafika: Strach z Huaweie. Západ burcuje kvůli špionáži, Čína vyrazila do protiútoku* [online]. Praha : Aktuálně.cz, 2019 [cit. 2019-03-01]. Dostupné z WWW: <http://zpravy.aktualne.cz/zahranici/huawei-prehledne-o-sporu/r~6464075a26011e996370cc47ab5f122>.

Ransomware jedna z největších současných hrozeb bude i nadále na vzestupu a stane se stabilním nástrojem pro útočníky. Při využití ransomware jako nabízenou službu se jeho dostupnost a rozšíření více zpřístupní široké škále kyberzločinců. Ransomware svou podstatou může zločincům sloužit i ke zrychlenému obohacení a zisku kryptoměny, protože výkupné se již nebude platit reálnými penězi ale právě pomocí kryptoměny. Platba v kryptoměně dále přispěje ke větší anonymizaci pachatelů.

Budoucí vývoj Internetové kriminality také zahrnuje šíření dětské pornografie a její přechod k živým přenosům. Tento problém umocní i rostoucí počet dětských uživatelů sociálních sítí. Sexuální predátoři se stávají technicky zdatní a hledají nové způsoby dosažení svých cílů. Hledají také nové cesty k organizování se do malých skupin, aby si zvýšili šanci na uniknutí před OČTŘ. I tito pachatelé se snaží využívat mobilní messaging se zabezpečením end-to-end.

Kriminalita na Darknetu se rozšiřuje do mnoha oblastí a zahrnuje široké pole kriminálních aktivit. Také mezi finančními podvody je očekáván nárůst. Přístup třetích stran k bankovním účtům a prodej uživatelských hesel, čísel karet a pinů nabírá na rozmachu. Poroste zneužívání internetu k šíření nepravdivých informací (fake news). Nevyhnutelný je i další růst ilegálních marketů i přes tvrdé postihy a vypínání za pomocí policie, soudů i jiných Evropských, nebo národních nařízení nelze než očekávat všeobecný rozmach kybernetické kriminality páchané na Internetu. Ještě stále si myslíte, že Vás se to netýká?

Paní Bosco z výzkumného institutu meziregionálního zločinu a spravedlnosti Spojených národů (UNICRI) se k budoucnosti kybernetické kriminality vyjádřila takto: „Pohled do budoucnosti spojuje nové technologie, jako jsou kvantové počítače, bločenku[61], robotiku, umělou inteligenci a strojové učení, ale zároveň představuje rozšíření oblastí zranitelnosti a prostor k páchání trestných činů, z tohoto spojení ale může vzájemně těžit veřejný i soukromý sektor. Přípravy na dvojí používání (zákonné i nezákonné) těchto technologií a navrhování mechanismů v oblasti bezpečnosti a odpovědnosti či odolnosti vůči manipulaci pomohou maximalizovat přínos těchto technologií a současně minimalizovat rizika pro občany a vlády.“[62]

[61]*Blokchain* [online]. San Francisco (CA) : Wikimedia Foundation, 2001 [cit. 2019-01-14]. Dostupné z WWW: < https://cs.wikipedia.org/wiki/Blockchain >.
[62]EUROPOL. *IOCTA: Internet Organised Crime Threat Assessment* [online]. Europol : European Cybercrime Centre, 2018 [cit. 2019-01-20]. Dostupné z WWW: <www.europol.europa.eu>.

5.2 Ostatní možné trendy

„Velká data (angl. Big data) je termín aplikovaný na soubory dat, jejichž velikost je mimo schopnosti zachycovat, spravovat a zpracovávat data běžně používanými softwarovými nástroji v rozumném čase. Pojem „velikost“ dat je chápán nejen z hlediska objemu dat měřeného giga-, tera- či petabyty, ale i z hlediska rychlosti jejich tvorby a přenosu a z hlediska různorodosti jejich typů.“[63] Korelace těchto dat umožňuje analytickým firmám odhadovat různé budoucí trendy. Zrychlení korelace umožní šetřit peníze za letenky, předpovídat výskyt chřipky a zjistit, které kanály nebo přeplněné budovy kontrolovat, když se potýkáme s nedostatkem zdrojů. Systémy založené na předpovědích získaných díky korelacím mohou v reálném čase překládat do cizích jazyků nebo automaticky řídit automobily.[64]

Z pohledu kybernetické kriminality mohou Big data mít zásadní vliv na vedení útoků. Jejich využití je a nadále bude v běžném životě výhodou, která se ovšem při neopatrné manipulaci, špatném sběru nebo útoku na data centra může obrátit v nevýhodu. Současně lze o využití pouze spekulovat, až čas ukáže, jak moc se sběr těchto dat bude vyplácet i kybernetickým zločincům.

5.2.1 Cloudové služby

Použití Ransomware je dnes v oblibě, blíží se však doba, kdy jeho použití narazí na své limity a útočníci začnou hledat nové způsoby. Jako další na řadě budou cloudové služby, v nichž se shromažďuje stále větší množství dat. Útok a následné selhání jediného datového centra najednou způsobí obtíže velkému množství podniků, státních agentur, provozovatelů kritické infrastruktury nebo i zdravotnických systémů. Pro podvodníky zde existuje šance na zisky v řádech miliard dolarů. Útočníci se budou cíleně zaměřovat na vyhledávání zranitelností cloudových služeb.

5.2.2 Technické prostředky

Také technické prostředky se neustále zdokonalují a zlepšují. V budoucnu lidstvo ke zlepšení, zefektivnění nebo nahrazení každodenních činností použije technické prostředky typu dronů, robotů, autonomních vozidel apod. Na tyto prostředky

[63] *Big data. Nové způsoby zpracování a analýzy velkých objemů dat.* [online]. Praha : CCB, 2011[cit. 2018-12.12]. Dostupné z WWW: <https://www.systemonline.cz/clanky/big-data.htm>.
[64] MEYER-SCHÖNBERGER, V., CUKIER, K. *Big Data.* Brno, 2014, s. 207.

bude kladen velký důraz a všechny budou mít přístup k Internetu. K jejich zneužití ze strany pachatelů zaručeně dojde.[65]

5.2.3 Umělá inteligence

Umělou inteligenci (angl. AI – Artificial Intelligence) budou pro své vlastní účely využívat i kybernetičtí zločinci. Namísto botnetu, jak jej známe dnes, začnou útočníci více využívat jejich sofistikovanější podoby. Clustery kompromitovaných zařízení, označované termínem hivenet nebo swarmbot (česky úly, roje) budou poháněné umělou inteligencí. Taková síť bude decentralizovaná. Bez lidského zásahu dokáže sdílet informace a pátrat po zranitelných cílech. Automaticky reagující systémy budou schopny rychlého rozšiřování i adaptivní reakce na obranná opatření. Útoky budou probíhat obrovskou rychlostí a zranitelné body budou často napadány současně a z více směrů. Lze očekávat zvyšující se množství soubojů různých typů malwaru mezi sebou, přičemž tato válka bude jen v omezené míře přímo řízena lidmi.[66]

5.2.4 Hypotetické možnosti

Možností zneužití umělé inteligence je celá řada. Pachatelé by mohli uzpůsobit systémy umělé inteligence používané v technických prostředcích pro vyprovokování srážek a cíleného útoku na svou oběť. Podle ředitele střediska z Cambridgeské univerzity Seána Ó Éigeartaigha by se mohla s větším zneužitím umělé inteligence zvýšit zejména počítačová kriminalita. Větší záběr by mohly představovat i útoky pomocí tzv. spear phishingu. Toto je podvodná technika používaná na Internetu k získávání citlivých údajů od konkrétní osoby. Velké nebezpečí vidí Seán Ó Éigeartaigh v možném zneužití umělé inteligence v politice. Jednotlivci a skupiny se snaží zasahovat pomocí Internetu do demokratických voleb (viz kauza Cambridge Analytica).

Umělá inteligence bude sloužit i k výrobě falešných a velmi realistických videí, která by mohla být použita k diskreditaci politických činitelů.[67] Její možnosti jsou už dnes na velmi dobré úrovni. Tyto videa se nazývají Deep Fake. „V současné době se tento trend usadil v oblasti politiky a my jste tak mohli vidět falešná videa Angely Merkelové, Donalda Trumpa nebo Baracka Obamy. Falešné video již zmiňovaného

[65]PIKORA, A. *Umělá inteligence ve službách útočníků.* [online]. Praha : Nitmedia, 2018 [cit. 2018-12-14]. Dostupné z WWW: < https://www.itbiz.cz/clanky/umela-inteligence-ve-sluzbach-utocniku>.
[66]PIKORA, A. *Umělá inteligence ve službách útočníků.* [online]. Praha : Nitmedia, 2018 [cit. 2019-01-23]. Dostupné z WWW: < https://www.itbiz.cz/clanky/umela-inteligence-ve-sluzbach-utocniku>.
[67]*Stinná stránka umělé inteligence, stroje pomáhají kyberzločincům* [online]. Cambridge : Novinky.cz, 2018 [cit. 2018-12-30]. Dostupné z WWW: <https://www.novinky.cz/internet-a-pc/bezpecnost/464210-stinna-stranka-umele-inteligence-stroje-pomahaji-kyberzlocincum.html>.

Baracka Obamy vyvolalo největší rozruch. Doposud se jednalo o více méně amatérské kousky z výukových aplikací. Toto video je však natolik věrohodné, že nad ním žasnou i odborníci. Nová technologie dokázala, že kdokoliv, kdo se někdy objeví na kameře, může promlouvat vaším hlasem. Odborníci výměnu tváří považují za neetickou a nebezpečnou. Odhaduje se, že v průběhu dvou až tří let může představovat velký problém. Sestavit výkonný software, který by dokázal falešná videa poznat, se zatím nepodařilo. Proto je potřeba o těchto manipulativních technikách vědět a být na ně připraveni.“[68]

6 Kybernetická kriminalita zaměřená na finanční škody

Cílem kapitoly je rozbor kybernetické kriminality, která se zaměřuje na finanční škody. V dnešní době je na vzestupu speciální druh malwaru. Tvůrci malware jsou jedni z nejvíce aktivních kyberzločinců na Internetu. Jejich cílem je opustit komplikované modely průniků do informačních systémů či k uživatelům a získávat peníze co nejsnazší cestou s pokročilou automatizací jejich práce.

„Ransomware (vyžadování výkupného) je typ malwaru, jehož prostřednictvím útočník vyžaduje pod různými výhružkami peníze, v lepším případě se na počítači může zobrazovat výzva k zaplacení „pokuty“ za údajné porušení autorských práv nebo používání nelegálního softwaru, v horším případě dojde k zašifrování dat na disku (přičemž není jisté, že po zaplacení útočník data odblokuje).“[69]

Ransomware je typický příklad pro šíření škodlivého kódu pomocí drive-by-download. To znamená, že na koncové technické prostředky se dostává už při pouhé návštěvě kompromitované webové stránky. Jeho zákeřnost spočívá v tom, že se může nacházet i na bezpečných webových stránkách, které zobrazují reklamu a pomocí ní se po kliknutí na reklamní banner dostane na cílový technický prostředek.[70] Tento malware napadá především operační systémy společnosti Windows a mobilní zařízení s OS Android. Nejsou to ale jenom operační systémy. Pro pachatele jsou lákavé i databázové servery.

První verze ransomware pouze zabraňovaly operačnímu systému ve spuštění a vyžadovaly platby přes SMS. Jejich hlavní nevýhodou byla snazší dohledatelnost

[68]*BUCNOST FAKE NEWS: Deep fake videa* [online]. Praha : Manipulátoři.cz, 2019 [cit. 2019-02-20]. Dostupné z WWW: <https://manipulatori.cz/budoucnost-fake-news-deep-fake-videa/>.
[69]KRÁL, M. *Bezpečný internet. Chraňte sebe i svůj počítač.* Praha, 2015, s. 14.
[70]ŠULC, V. *Kybernetická Bezpečnost.* Plzeň, 2018, s. 49.

pachatelů. Popularitu ransomware nastartovala existence kryptoměn, čímž se značně pro OČTŘ snížila šance na odhalení pachatele. Stejně jako se v čase vyvíjí kybernetická kriminalita, vyvíjí se i ransomware. Od symetrického šifrování přešel do asymetrického s různými variantami klíče.

Prvním ransomware byl v roce 1989 trojan AIDS, který šifroval pevný disk uživatelům hledající informace o viru HIV a požadoval po nich platbu na Panamský účet v ceně 189 – 378 dolarů za dešifrování HDD. V roce 2017 už byl zaznamenán masivní a celosvětový útok ransomwarem WannaCry v počtu 45 000 útoků v 74 zemích světa včetně ČR. Ve Velké Británii tento útok vyřadil z provozu počítače v nemocnicích a jiných specializovaných zařízeních a donutil jejich správce a vedení nemocnic k zaplacení, aby došlo k dešifrování a návratu do původního stavu.[71]

6.1 Ransomware policejní virus

V roce 2012 Policie ČR varovala občany, že zaznamenala zvýšený výskyt případů, kdy docházelo k šíření ransomwaru. Kyberútok spočíval nejen v šíření ransomwaru, ale i v podvodném požadování peněz od internetových uživatelů.[72] Tento ransomware se zaštiťoval Policií ČR a napadený počítač přes celou obrazovku zobrazil výzvu Policie ČR s oznámením směrem k uživateli, že se dopustil trestného činu a proto byl jeho počítač zablokován. Pokud do 48 hodin zaplatí 2000 Kč pomocí kuponu Ukash nebo PaySafeCard, bude uživatel z trestného činu vykoupen.[73]

6.1.1 Reverzní analýza

Reverzní analýzu ransomwaru Policie ČR provedl bezpečnostní tým CESNET-CERTS a jeho forenzní laboratoř FLAB. Analýza byla provedena z obrazu disku napadeného počítače a operační paměti. Laboratoř odchytila síťový provoz zachycující průběh zadání platebního kódu.[74]

Reverzní analýzou byl ransomware nejprve dekódován a pak pomocí nástrojů pro reverzní inženýrství důkladně analyzován. K analýze byly použity dva nástroje OllyDbg a IDA Pro. Bylo zjištěno, že se skládá ze dvou nezávislých částí. První z nich

[71]SMEJKAL, V. *Kybernetická kriminalita*. Plzeň, 2018, s. 214.
[72]TOPINKOVÁ, M. *Policie varuje před počítačovým virem, který se šíří internetem v Česku* [online]. Praha : iDnes.cz, 2012 [cit. 2018-12-10]. Dostupné z WWW: <https://www.idnes.cz/zpravy/cerna-kronika/sireni-pocitacoveho-viru.A121008_144459_domaci_maq>.
[73]*Ransomware – „policejní virus“ na pitevním stole* [online]. Praha : ROOT.CZ, 2013 [cit. 2018-12-11]. Dostupné z WWW: <https://www.root.cz/clanky/ransomware-policejni-virus-na-pitevnim-stole/>.
[74] *Ransomware – „policejní virus“ na pitevním stole* [online]. Praha : ROOT.CZ, 2013 [cit. 2018-12-11]. Dostupné z WWW: <https://www.root.cz/clanky/ransomware-policejni-virus-na-pitevnim-stole/>.

je klient botnetu, který napadený počítač přemění v zombie a zapojí jej do příslušného botnetu a dále čeká na příkazy z C&C (Command and Control) serveru. Druhou částí je vlastní aplikace vyžadující platbu.[75]

6.1.2 Napadení systému

K tomu, aby mohl být uživatelův počítač napaden, vedla poměrně dlouhá cesta. Útočníci nejprve napadli webové stránky nejčastěji s obsahem pro dospělé. Tyto stránky sloužily jako vstupní bod. Při vstupu uživatele na tyto stránky došlo k přesměrování na útočníky podvrženou webovou stránku s exploity, které útočníkům umožnily přístup do systému. U tohoto typu ransomware byly použity tři cesty možné infikace:

1) zavirovaný PDF soubor,

2) zneužití zranitelnosti Internet Exploreru a

3) zneužití zranitelnosti Java Virtual Machine.[76]

Slabinou všech ransomware, ale i virů obecně, je nutnost zajistit si své spuštění po restartu operačního systému. Tohoto spuštění je docíleno několika způsoby:

- použití práv uživatele systému případně práv administrátora,
- zápisem nových hodnot do registru systému,
- vnoření EXE souboru s virem do složky „Po spuštění“,
- pomocí plánovače úloh systému,
- vytvořením nové služby nebo driveru do jádra systému.

„Policejní“ ransomware využíval registrové klíče. Konkrétně byl spuštěn proces rundll32.exe, který se odvolal na vstupní bod v knihovně malwaru wlsidten.dll a pro jistotu se zapsal i do složky „Po spuštění“.[77]

[75] *Ransomware – „policejní virus“ na pitevním stole* [online]. Praha : ROOT.CZ, 2013 [cit. 2018-12-11]. Dostupné z WWW: <https://www.root.cz/clanky/ransomware-policejni-virus-na-pitevnim-stole/>.
[76] *Ransomware – „policejní virus“ na pitevním stole* [online]. Praha : ROOT.CZ, 2013 [cit. 2018-12-11]. Dostupné z WWW: <https://www.root.cz/clanky/ransomware-policejni-virus-na-pitevnim-stole/>.
[77] *Ransomware – „policejní virus“ na pitevním stole* [online]. Praha : ROOT.CZ, 2013 [cit. 2018-12-11]. Dostupné z WWW: <https://www.root.cz/clanky/ransomware-policejni-virus-na-pitevnim-stole/>.

Po úspěšném napadení a zavedení ransomware do systému je jeho dalším krokem udržet se v napadeném počítači a zkomplikovat své odstranění. Začíná boj proti antivirovému programu. Pokud antivirový program nemá aktualizované definice a typ nákazy nezná, není schopen jej detekovat. V opačném případě se ransomware pokusí vypnout antivirovou ochranu počítače, nebo změnit její oprávnění, případně změnit oprávnění k přístupu k souborům s ransomware obsahem. Druhým soupeřem je administrátor, nebo znalý uživatel.

Popisovaný policejní ransomware blokoval správce úloh ve svém spuštění. Neustále obnovoval zápis v registrech a tím zamezoval svému smazání. A před antivirovým programem se chránil zakódováním klíčové knihovny, která byla stažena do počítače po navštívení napadených stránek a uložená na HDD.

Komunikace s botnet klientem probíhala v co možná nejméně nápadném režimu vložením vlastního kódu do spuštěné instance webového prohlížeče, který komunikoval s C&C serverem na portu 80 (běžný komunikační port). Webový prohlížeč byl netypicky spuštěn na pozadí v tzv. virtuální ploše. Komunikační proces probíhal samostatně a synchronizace s ostatními součástmi ransomware byla prováděna pomocí odkládacího souboru. V tomto konkrétním případě se jednalo o soubor "%allusersprofile%/Data aplikaci/netdislw.pad". Komunikace probíhala na předem určenou IP adresu C&C serveru, ale ransomware měl v sobě uloženy ještě další záložní IP adresy v případě nenavázání komunikace.

6.1.3 Samotná aplikace

Pod obrazovkou, kterou uživatel viděl (viz obrázek 7), se skrývala samostatná aplikace (ransomware) vytvořená v programovacím jazyku Borland Delphi. Na počítač byl ransomware stažen klientem botnetu a uložen do odkládacího souboru, aby mohlo dojít k jeho aktualizaci. Ransomware byl spuštěn klientem botnetu při každém startu počítače v režimu always-on-top.

Postižený uživatel byl zobrazen v oznámení ransomwaru za pomocí webové kamery (pokud byla přítomna) spolu s aktuální zemí, oblastí, doménového jména, místa a IP adresy. Zobrazované údaje se mohly lišit v závislosti na nastavení ransomware. Dále byl uživateli zobrazen text „Váš počítač (prohlížeč) byl uzamčen" a výpis z trestných činů, kterých se uživatel údajně dopustil. Psychologický efekt na uživatele,

který surfoval na stránkách s obsahem pro dospělé je umocněn jeho obrazem z webové kamery a výpisem údajné trestné činnosti.

Ransomware testuje zadání PIN kódu tak, aby byla zaručena jeho pravost. Pro Ukash je to kód obsahující 19 znaků a vždy začíná 633718 a pro PaySafeCard je délka znaků 10 číslic a počáteční znak je vždy 0. Získaná čísla jsou botnetem odeslána na C&C server a znovu ověřena u poskytovatelů platebních služeb.[78]

Obrázek 7: Policejní ransomware[79]

6.1.4 Odstranění ransomwaru

Odstranění ransomwaru probíhá v několika krocích. Nejdříve je potřeba identifikovat hrozbu, poté zlikvidovat její obranné mechanismy a lokalizovat napadené soubory, které se musí z PC odstranit. Je nutné prohledat počítačové registry, složku „Po spuštění“, plánovač úloh, běžící služby, smazat internetovou cache z prohlížečů, dočasné soubory atd. Postup odstranění je složitý proces, který je nejlépe komunikovat s odborníkem. Někdy je jediným řešením smíření se s kompletní ztrátou dat a reinstalace operačního systému.

[78] *Ransomware – „policejní virus“ na pitevním stole* [online]. Praha : ROOT.CZ, 2013 [cit. 2018-12-11]. Dostupné z WWW: <https://www.root.cz/clanky/ransomware-policejni-virus-na-pitevnim-stole/>.
[79] *Ransomware – „policejní virus“ na pitevním stole* [online]. Praha : ROOT.CZ, 2013 [cit. 2018-12-11]. Dostupné z WWW: <https://www.root.cz/clanky/ransomware-policejni-virus-na-pitevnim-stole/>.

6.2 WannaCry

V dubnu a červnu 2017 zasáhly útoky ransomwarů WannaCry a Petya tisíce společností na celém světě. Způsobily snížení produktivity a škody za více než 4 miliardy amerických dolarů.[80] WannaCry obsahoval jazykové mutace a zasáhl i počítače v ČR. Během 24 hodin bylo zaznamenáno více než 100 000 napadených počítačů ransomwarem WannaCry. Ransomware se kromě emailových příloh šířil po lokálních sítích organizací, do kterých pronikl. Při průniku do počítače zobrazil informaci o šifrování dat pevného disku a informaci o platbě výkupného spolu s časem, kdy bude cena za dešifrování počítače zvednuta.

Obrázek 8: WannaCry[81]

Jak již bylo napsáno WannaCry se šířil emailem, který obsahoval přílohu podobnou ZIP archivu. Po otevření přílohy byl spuštěn program, který do počítače nainstaloval samotný ransomware. K průniku do systému využil ransomware známého exploitu operačního systému Windows. Ransomware se dokázal dále šířit za pomocí vlastní botnetové sítě, ale i nezabezpečených počítačů v síti. Botnetová síť hledala dostupné IP adresy zranitelných počítačů a snažila se o instalaci svých knihoven na tyto

[80] *WannaCry a Petya způsobily škody za více než 4 miliardy dolarů* [online]. Praha : ROOT.CZ, 2017 [cit. 2019-01-11]. Dostupné z WWW: <https://www.root.cz/zpravicky/wannacry-a-petya-zpusobily-skody-za-vice-nez-4-miliardy-dolaru/>.

[81] *WannaCry* [online]. Redwood City (CA) : AVAST.COM, [cit. 2019-02-01]. Dostupné z WWW: <https://www.avast.com/cs-cz/c-wannacry>.

PC. Napadeným počítačům byly zašifrovány soubory a složky na pevném disku. Zašifrované soubory měly přílohu WCRY.

WannaCry se zaměřuje na soubory s příponami DOC, PPT, XLS, JPG, PNG, TIFF, videosoubory, ale také na projekty a zálohy operačního systému.

Cena za dešifrování dat byla požadována v Bitcoinech (kryptoměna) a nastavena v přepočtu na 200 USD. Ransomware ale neustával se svou činností a po uplynutí stanoveného času dvojnásobně zvyšoval cenu za dešifrování dat. Dále oznamoval, za jak dlouho již nebude dešifrování možné.

6.3 Směr vývoje

V poslední době je v rámci crime-as-a-service nabízena možnost nadefinovat si vlastní ransomware (RaaS). Zadavateli je pak poskytnuta veškerá logistická a programátorská podpora. Při využití nabízených služeb, objednavatel zaplatí dohodnutou cenu v kryptoměně. Dle dostupných informací je cena za tuto „službu“ ve stovkách dolarů. Obchodní model je autory ransomware nastaven na podíl ze zisku celé kampaně. Na marketech Darknetu v doméně ONION je dostupný formulář k vytvoření takto personalizovaného ransomware (Satan). Satan nevyžaduje žádný počáteční poplatek za zakoupení. Poplatky jsou stanoveny na 30% z výkupného. Satan může obsahovat i jazykové mutace a je zaměřen i na neznalého uživatele.[82] Průměrnou cenou výkupného v roce 2016 bylo 679 amerických dolarů. Cena za dešifrování je ale závislá na kupní síle a movitosti oběti. Ransomware je pro útočníky miliardovým byznysem.

Nejúčinnější obranou je zálohování dat na více místech, přemýšlet u vykonávané práce a nestahovat ani nespouštět software z neznámých zdrojů.[83]

Ransomware budoucnosti bude cílen proti chytrým mobilním zařízením, televizím nebo věcem, které budou připojeny k Internetu v rámci IoT.[84]

[82]*Ransomware je na vzestupu, vydírání si můžete objednat* [online]. Praha : ROOT.CZ, 2017 [cit. 2019-02-01]. Dostupné z WWW: <https://www.root.cz/clanky/ransomware-je-na-vzestupu-uz-laka-i-amaterske-kyberzlocince/>.
[83]*Ransomware je na vzestupu, vydírání si můžete objednat* [online]. Praha : ROOT.CZ, 2017 [cit. 2019-02-01]. Dostupné z WWW: <https://www.root.cz/clanky/ransomware-je-na-vzestupu-uz-laka-i-amaterske-kyberzlocince/>.
[84]KOLOUCH, J. *Cybercrime*. Praha, 2016, s. 229-230.

6.4 Dílčí závěr

Ransomware není jediným prostředkem, který pachatelé kybernetické kriminality používají k trestné činnosti v prostředí Internetu a která je zaměřená na finanční zisk. V dnešní době má ale jeho užití stoupající tendenci. Ruku v ruce s tímto poznatkem jde fakt, že se jeho operační nasazení zjednodušilo a jeho použití už není závislé na odbornících, ale ransomware útok si může skrze markety a službu ransomware-as-a-service objednat i naprostý ICT laik. Popularita rodiny ransomware se tedy každým rokem zvětšuje a zahrnuje nové přírůstky. Nebezpečnost je také v diferenciaci rodiny ransomware. Některé druhy uzamknou počítač, jiné zamezí uživateli v přístupu k datům, další obtěžují uživatele výhružnými zprávami. Podle Smejkala rozlišujeme tři druhy ransomware: šifrovací, nešifrovací a doxware.[85]

V budoucnosti se část kybernetických zločinců zaměří na těžbu kryptoměn a přizpůsobí malware do takové podoby, aby tyto útoky usnadnil a zasáhl co největší množství počítačů. Rozsáhlý botnet s mnoha počítači a jejich výpočetním výkonem těžbu kryptoměn značně usnadňuje a hlavně urychluje. Oběti navíc nemusí mít povědomí o tom, co jejich počítač dělá, když procesorový výkon není právě využíván.

Zaměření pachatelů bude směřovat i na mobilní telefony a jejich aplikace. Hrozby v oblasti kolem mobilních telefonů se rok od roku zvyšují a počet mobilního malware vzrostl v roce 2017 o 54%. Ten samý rok bylo každý den zablokováno v průměru 24 000 nebezpečných mobilních aplikací.[86] Ransomware ale zřejmě zůstane v popředí zájmu pachatelů díky nesnadné identifikaci pachatele, vyděračské a zastrašující povaze, psychologickým a jiným neetickým výhodám.

Útok typu WannaCry způsobil v celosvětovém měřítku obrovské škody a donutil nemocnice za odblokování svých počítačů vyděračům zaplatit. Jednoduchost v použití tohoto nástroje a jeho hlavní účel by měl pro uživatele být alarmující. Ve vlastním zájmu by každý uživatel měl mít základní znalosti o obraně proti tomuto nástroji. Uživatelé, kteří přemýšlejí o svých aktivitách v kybernetickém prostředí, používají základní metody práce s PC a uzpůsobují své chování v prostředí Internetu, se stávají pro pachatele překážkou, které je lepší se vyhnout.

[85]SMEJKAL, V. *Kybernetická kriminalita*. Plzeň, 2018, s. 214.
[86]*Executive Summary. 2018 Internet Security Threat Report* [online]. Mountain View : Symantec, 2018 [cit. 2019-02.02]. Dostupné z WWW: <https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf>.

7 Kybernetická kriminalita zaměřená na psychické škody

Psychické škody může pachatel na své oběti napáchat už jen útokem na technický prostředek. V této kapitole je ale rozebrána mnohem vážnější a velmi nebezpečná forma trestné činnosti. Jedná se o kybernetickou šikanu. Stejně jako v našem fyzickém světě i ve virtuálním světě dokáže šikana napáchat neskutečné škody a velmi vážně poškodit oběť. Šikana ve fyzickém světě spočívá ve snaze útočníka poškodit, ublížit, zesměšnit, urazit ať již fyzicky nebo psychicky. Toto jednání se pak přenáší do prostředí kyberprostoru, kde se stává stejně nebo i více nebezpečným.

7.1 Kyberšikana

„Aby bylo možné hovořit o kyberšikaně, je nutné, aby oběť byla napadena cíleně a opakovaně jedincem nebo skupinou. V některých případech je kyberšikana spojena s klasickou šikanou, která zahrnuje například fyzické útoky, slovní nadávky, pomluvy nebo ponižování. Kyberšikana zahrnuje několik forem útoku, kterými mohou být verbální útoky, ztrapňování šířením fotografie, videa nebo zvukové nahrávky, vyhrožování a zastrašování, krádež identity, průnik na účet s cílem dehonestovat oběť, vydírání nebo i obtěžování vyzváněním.“[87] Kyberšikana se již netýká pouze počítačů, zločinci útočí na mobilní telefony svých obětí (obtěžujícími textovými zprávami, vyzváněním, atd.), na sociální sítě apod. Kybernetická šikana se nevyhýbá ani známým osobnostem.

7.2 Druhy kyberšikany a její prostředky

Rozsáhlost kyberprostoru dává kyberšikaně nečekané rozměry. I jediný obrázek ze sociální sítě se dokáže šířit k miliónu uživatelů. Kontrolu nad tím, kdo a jak s obrázkem nakládá lze jen těžko uplatňovat. Kyberšikaně se nejlépe daří mezi dětmi a mladými lidmi, kteří v dnešní míře až nadužívají výpočetní techniku. Je potřeba, aby se o kyberšikaně mluvilo nejen doma, ale i ve vzdělávacích institucích, zájmových kroužcích a sdruženích, kam děti a mladí lidé docházejí, nebo kde se zdržují.[88] Formy a prostředky kyberšikany nesouvisí vždy přímo s kyberprostorem. Někdy to mohou být obtěžující textové zprávy nebo telefonáty. Tyto formy zde vzhledem k možnostem a rozsahu práce nejsou dále rozebírány.

[87]ROGERS, V. *Kyberšikana. Pracovní materiály pro učitele a žáky i studenty.* Praha, 2011, s. 62.
[88]ROGERS, V. *Kyberšikana. Pracovní materiály pro učitele a žáky i studenty.* Praha, 2011, s. 32 – 33.

7.2.1 Prostředky

Email – využití tohoto prostředku je jedním z nejzákladnějších a nejjednodušších. Útočník rozesílá útočné, šokující a jinak škodlivé emaily většinou za použití falešné emailové schránky. Má neomezené možnosti k vytváření dalších falešných schránek. [89]

Chatroom – chatovací místnosti jsou již na ústupu, nahrazují je sociální sítě. Přesto se takové místnosti nebo uživatelská fóra ještě najdou. Útočníci zde vystupují pod falešnými identitami a mohou zde být přítomni i ve větším počtu. Vyhlédnou si osobu (náhodně, cíleně) a svými útoky na ni jí znepříjemňují pobyt na fóru.

Instant messaging - užíván podobně jako obtěžující textové zprávy. Pro útočníka zde není jednoduché skrýt svou anonymitu. Některé aplikace umožňující instant messaging totiž vyžadují zadání telefonního čísla ke spárování s vytvářeným účtem. Tento formát je zastoupen například Skypem, Facebook messaging atd. Je nutné, aby útočník investoval finanční prostředky k nákupu kreditů a SIM karty.

Sociální sítě – tyto služby jednoduše propojí uživatele mezi sebou a umožňují jim sdílení fotografií, videí a jiných dat. Tyto uživatelské výhody jsou útočníci schopni proměnit v nevýhody. Fotky a videa mohou být použity k vydírání, zprávy k šíření pomluv a nepravd. Oběti většinou ani nepřemýšlí, komu vlastně udělují „přátelství“. Vytvořit si falešný účet nevyžaduje žádnou speciální znalost Internetového prostředí. Sociální sítě umožňují agresorům také velice snadno sledovat jejich oběti.

Internetové stránky – útočníci si běžně vytvářejí hanlivé blogy a jiné webové stránky o svých obětech. Prostřednictvím sociálních sítí a jinými prostředky jsou schopni tyto stránky propagovat a šířit mezi uživateli. Mnoho webových stránek lze vytvořit s minimálními finančními náklady nebo dokonce zadarmo. Na těchto stránkách se pak přímo nabízí možnost vytvoření ankety s otázkami zaměřenými na oběť.

[89] ROGERS, V. *Kyberšikana. Pracovní materiály pro učitele a žáky i studenty.* Praha, 2011, s. 34.

Obrázek 9: Druhy kyberšikany[90]

Druh	Popis
Nářez (Flaming)	Internetové diskuze za pomocí elektronických zpráv, které používají agresivní a útočný jazyk.
Obtěžování (Harassment)	Opakované posílání útočných, urážlivých nebo nevyžádaných zpráv.
Pomlouvání (Denigration)	Rozšiřování pomluv, drbů a lží o někom s cílem poškodit jeho pověst nebo vztahy.
Předstírání (Impersonation)	Posílání komentářů apod. pod cizí identitou.
Prozrazení (Outing)	Sdělování cizích tajemství a citlivých dat bez souhlasu dotyčných.
Podvod (Trickery)	Přesvědčení obětí k prozrazení tajemství nebo citlivých dat a následné zveřejnění v Internetu.
Vyloučení (Exclusion)	Cílené vyloučení z online komunity nebo skupiny.
Kyberpronásledování (Cyberstalking)	Opakované a intenzivní obtěžování a ponižování, které zahrnuje výhrůžky nebo zastrašování.

7.3 Znaky kyberšikany

Mezi hlavní znaky kyberšikany je možné podle Koloucha zařadit: [91]

- pocit anonymity (útočník nabývá názoru, že je na Internetu nedohledatelný),
- neomezenost útoku (díky ICT nemusí útočník řešit ani čas ani prostor, je možné šikanovat kdykoliv, odkudkoliv a kdekoliv s mnohem menším úsilím),
- neomezený okruh útočníků (ve virtuálním světě nezáleží na věku, pohlaví, fyzické síle, postavení, šikanujícím může být kdokoliv),
- neomezený prostor a prostředky (lze opakovaně vyvěšovat urážlivé poznámky, komentáře, fotografie, videa na různých portálech, sociálních sítích aj. a tyto materiály lze dále rozvíjet),
- obtížná zjistitelnost (kybernetickou šikanu většinou nedoprovází fyzické následky, jako jsou podlitiny, chybějící peníze aj.),
- trvalost.

[90]ROGERS, V. *Kyberšikana. Pracovní materiály pro učitele a žáky i studenty.* Praha, 2011, s. 35.
[91]KOLOUCH, J. *Cybercrime*. Praha, 2016, s. 310.

V prostředí Internetu, za maskou anonymity se lidé chovají jinak, než v reálném světě. O své osobě, věku a pohlaví mohou beztrestně lhát a na jejich lež nemusí být lehké přijít. Díky těmto lžím, falešným identitám a dalším podvodům je snadné zmást protistranu, zvláště ty osoby, které se v prostředí Internetu chovají neopatrně. Útočník svou oběť může napadnout pouze jednou a o další šíření kyberšikany se postarají jiní uživatelé. Kyberšikana je spojena především s psychickým týráním obětí, které nelze snadno rozeznat. Lidé jen neradi ostatním sdělují, že se stali obětí kyberšikany.

7.4 Hledám kluka z autobusu

Moderní technologie nám dávají možnost sdílet zážitky mezi uživateli Internetu. Nemusí se přitom jednat pouze o přátele. V tomto konkrétním případě se nahraný obsah stal terčem posměšků právě od neznámých lidí, kteří navíc obsah dále šířili. Mladá dívka na Internet nahrála video, v němž hledá kluka, kterého potkala v autobuse. Video obsahovalo detailní popis chlapce a autobusu, kterým dívka jela. Dívka popsala například i tašku, kterou hledaný hoch nesl. Dále zveřejnila své telefonní číslo s prosbou ohledně kontaktu, pokud se někomu hledaného chlapce podaří najít. Nevědomky tak vytvořila video inzerát, který se stal hitem českého internetu. Dle dostupných informací video za tři měsíce nasbíralo přes 33 tisíc zhlédnutí. Jakmile se video mezi uživateli internetu stalo populární, nešlo již zastavit lavinu jeho šíření. V komentářích pod videem se strhla lavina nadávek, komentářů k jejímu vzhledu, přednesu a podání. K popularitě videa přispělo i jeho provedení a autentičnost. Video začalo na Internetu žít „vlastním životem“ a dále bylo uživateli parodováno.

Video se dá na portále YouTube najít u různých uživatelů dodnes. Originální kanál dívky však byl z video portálu smazán a spolu s ním i veškerá její další videa. V prostředí Internetu se směrem k dívce strhla lavina kybernetické šikany, kterou již nešlo zastavit. Zveřejněné video dívce, které v té době bylo 9 let, zcela změnilo život. Ponížení nezažila jen v rámci kyberprostoru, ale také v reálném životě a mimo jiné byla nucena vyhledat lékařskou pomoc.[92] Rodiče dívky se situaci snažili řešit a aktivně se zapojili do odstraňování obsahu. [93] Motivace k nahrání podobných videí je zcela zřejmá. Zejména u dětí a mladých lidí jsou taková videa spojena s vidinou proslavení se (YouTubeři) nebo vážně myšlenými vzkazy.

[92]KOLOUCH, J. *Cybercrime*. Praha, 2016, s. 312.
[93]ROGERS, V. *Kyberšikana. Pracovní materiály pro učitele a žáky i studenty.* Praha, 2011, s. 64-65.

Obrázek 10: Odezva na zveřejněné video[94]

7.5 Další oběti a typy

Mezi první obětí kyberšikany byl Kanaďan Ghyslain Raza na internetu známý jako Star Wars Kid. Tento chlapec natočil sám sebe při předvádění bojové scény z filmu Hvězdné války. Spolužáci mu ale nahrávku ukradli a pro pobavení ostatních zveřejnili na Internetu. Ghyslan se psychicky zhroutil a dlouhodobě se léčil. [95]

Jeden z nejtragičtějších evropských případů byla sebevražda polky Anny Halman. Pět jejich spolužáků podrobilo Annu před třídou sexuální šikaně. Tuto scénu nahráli na mobilní telefon a vyhrožovali dívce jejím zveřejněním na internetu.[96]

Existují i útoky mířené na identitu uživatele. Útočník se při tomto typu útoku vydává za oběť s cílem poškodit její profil a pohled na ní v očích kamarádů, spolupracovníků nebo rodiny. „Většina strůjců kyberšikany si vystačí s tím, že své oběti urážejí a vyhrožují jim. Menší část z nich však jménem svých obětí páchá zločiny. V roce 2007 byla skupina bojující proti internetovému zločinu s názvem CastleCops napadena kýmsi, kdo zahltil jejich paypalový účet dotacemi z Podvodně používaných paypalových účtů. Oběti používající PayPal o prostředníkovi nevěděly. Viděly jen, že

[94]*Hledám kluka z autobusu* [online]. Praha : Zpovědnice, 2014 [cit. 2019-02-27]. Dostupné z WWW: <https://www.zpovednice.cz/detail.php?statusik=824724>.
[95]*Kyberšikana* [online]. Olomouc : Centrum PRVoK PdF UP, 2010 [cit. 2019-03-01]. Dostupné z WWW: <https://www.e-bezpeci.cz>.
[96]*Kyberšikana* [online]. Olomouc : Centrum PRVoK PdF UP, 2010 [cit. 2019-03-01]. Dostupné z WWW: <https://www.e-bezpeci.cz>.

jejich účty byly vybrané a peníze se posílaly na účet skupiny CastleCops. Reputace skupiny byla velmi poškozena.“[97]

7.6 Směry vývoje

Kybernetická šikana úzce kopíruje šikanu ve skutečném světě a její další prognózy jsou s touto šikanou úzce spjaty. Nadále bude růst počet dětí, které přijdou do styku s určitou formou kyberšikany. Na školách bude převládat forma posměšků a vydírání prostřednictvím sociálních sítí. Častější budou i stránky na sociálních sítích, speciálně zaměřované na zesměšňování oběti.

Společnost musí i nadále vyvíjet tlak na zákonodárce k vytvoření opatření, která kyberšikanu zmírní a zároveň donutí provozovatele sociálních sítí efektivněji bojovat proti jejím projevům a výskytu v prostředí jejich sítí i na Internetu.

7.7 Dílčí závěr

Většina útoků při kyberšikaně je dost přímočará. Útočníci se spojují do početných skupin ať už cíleně nebo ne. Prohlídka sociálních sítí dokáže odhalit spoustu skupin, které jsou plné nenávisti vůči jiným skupinám, nebo osobám. Tyto skupiny mají jedno společné (například chodí na jednu školu, nebo jsou z jednoho kroužku apod.). Sociální sítě tyto skupiny všemožně potlačují, zakazují a mažou, ale tato obrana je nedostatečná.

Časté případy kyberšikany ukazují alarmující skutečnost, která dokazuje souvislost mezi kyberšikanou a školní šikanou. Kybernetická šikana velice úzce souvisí s dalšími činy, které svým obětem působí psychické škody. Jedná se především o sexting (sdílení a zveřejňování citlivých materiálů v rámci Internetu), kybergrooming (online komunikace útočníka s cílem přimět protistranu, většinou dítě, k osobnímu setkání), rizikové seznamování v prostředí Internetu apod.

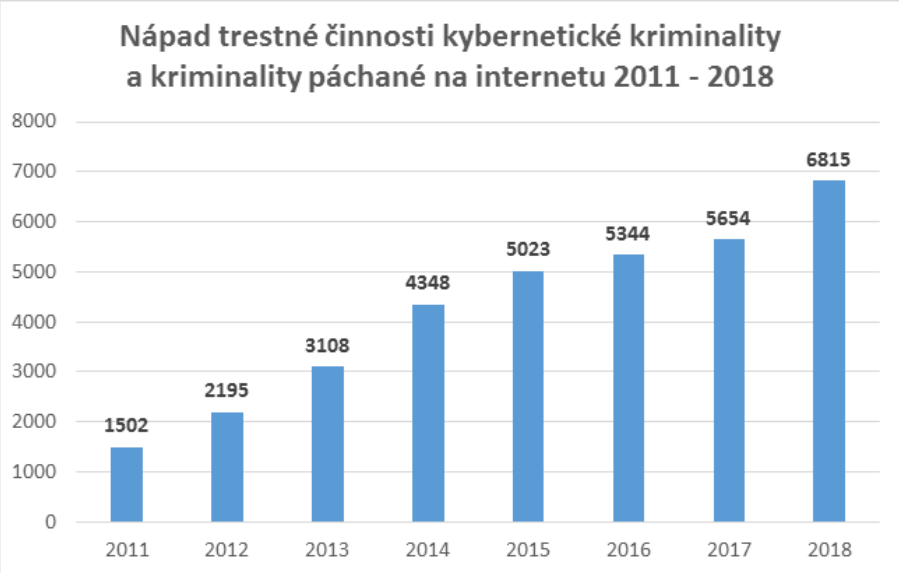
Obrana proti kyberšikaně není jednoduchá a ve spoustě případů nejde jednoduše uplatnit a nezbývá než čelit jejím následkům. K hlavním prvkům ochrany zde patří snaha dozvědět se o problematice co nejvíce a šířit nabité informace mezi dalšími rodinnými příslušníky a ve svém okolí. Pouze znalý a obezřetný uživatel může minimalizovat dopad této šikany na svou osobu, nebo se útoku zcela vyhnout.

[97]MCCARTHY, L., WELDON-SIVIY, D. *Bud pánem svého prostoru. Jak chránit sebe a své věci, když jste online*. Praha, 2013, s. 119.

8 Zhodnocení nárůstu kyberkriminality a její promítnutí do společnosti

Nárůst kybernetické kriminality se zaměřením na finanční škody je ve světě již zcela patrný a útoky typu WannaCry již zasáhly i některé počítače v České republice. Do budoucna se není možné těmto útokům vyhnout. V roce 2018 bylo Policií ČR v oblasti kybernetické kriminality a kriminality páchané na internetu evidováno 6815 trestných činů, což je ve srovnání s rokem 2017 nárůst o více než 1000 skutků.[98]

Obrázek 11: Nápad trestné činnosti kybernetické kriminality[99]



Dopad finanční kriminality za použití útoku ransomwarem je enormní a jeho hlavním motivem je finanční zisk. Vedlejšími motivy může být ukázka schopností, zastrašování, znemožnění funkce určitých systémů a jiné. Závažnost útoku se bude vždy odvíjet podle počtu zasažených technických prostředků (aktiv) a jejich důležitosti pro postižený subjekt.

Finanční kriminalita se odráží i v náladě společnosti. Úspěšné útoky a zaplacení výkupného nejsou vždy společností vnímány v pozitivním smyslu. Pokud obrana selhala a jedná se o klíčový prvek infrastruktury, je potřeba rozhodnutí o zaplacení výkupného veřejnosti náležitě zdůvodnit nebo utajit.

[98] *Kyberkriminalita* [online]. Praha : Policie ČR, 2019 [cit. 2019-02-22]. Dostupné z WWW: <www.policie.cz/clanek/kyberkriminalita.aspx>.
[99] *Kyberkriminalita* [online]. Praha : Policie ČR, 2019 [cit. 2019-02-22]. Dostupné z WWW: <www.policie.cz/clanek/kyberkriminalita.aspx>.

Téměř vždy je nutné vynaložit další náklady na obnovení chodu napadených aktiv do původního stavu a přijmout opatření, aby se podobné situace neopakovaly. Scénářů s možnými dopady na společnost je celá řada. Hlavním obranným prostředkem je informovaná odborná i laická veřejnost, aktualizované operační systémy i firmware jednotlivých zařízení a zálohování důležitých dat na několika místech. Probíhajícímu útoku se nedá vyhnout, ale pouze připravená obrana dokáže minimalizovat jeho dopady.

Také nárůst kyberšikany je alarmující. Každou chvíli je ve zprávách zveřejněn osud některých lidí, kteří se stali obětí kybernetické šikany ať už ze strany svých spolužáků, nebo od neznámých lidí. Rozdělení společnosti přispívá k poklesu morálních hodnot a tento pokles se mimo jiné projevuje i v prostředí Internetu.

Obrana proti cíleným útokům skupiny nebo jednotlivce na vytipované jedince není snadná a na obětech může zanechat velké psychické škody. Některé oběti může dohnat až k sebevraždě. Pomyslná anonymita v Internetu a možnost vydávání se za někoho jiného je silnou zbraní šikanujících. V oblasti prevence kriminality patří ČR v rámci Evropy mezi špičky. Vznikla zde tedy celá řada projektů, které se zabývají vzděláváním všech skupin uživatelů od dětí až po seniory. Jsou to například projekty Seznam se bezpečně, E-Bezpečí, Bezpečný internet, Linka bezpečí a různá krizová centra.[100]

8.1 Vývoj kybernetické bezpečnosti v ČR

Mnoho menších firem a státních organizací nemá zavedeno řízení kybernetické bezpečnosti, přesto že existují nejrůznější modely jejího řízení. Nízké povědomí uživatelů o bezpečnosti a chování v Internetu je důsledkem jejich slabého zájmu a přesvědčení, že útok na ně cílen nebude. Náklady na bezpečnost v ICT jsou velmi vysoké. ICT oddělení nejsou ziskovou položkou a firmy i státy se zdráhají vyšších investic do oblasti bezpečnosti ICT jako celku. Z různých průzkumů informační bezpečnosti vyplynulo, že vedoucí pracovníci jsou přesvědčeni, že jejich firma není pro útočníka dostatečně zajímavá a vedení kybernetického útoku je finančně nákladné. Z těchto faktů vyplývá přesvědčení, že pravděpodobnost útoku na jejich firmu je nízká.[101]

[100]KOŽÍŠEK, M., PÍSECKÝ V. *Bezpečně na internetu. Průvodce chováním ve světě online*. Praha, 2016, s. 144-152.
[101]ŠULC, V. *Kybernetická Bezpečnost.* Plzeň, 2018, s. 11.

Na zhoršující se vývoj v oblasti kybernetické bezpečnosti byla nucena reagovat i česká legislativa, která vydala zákon č. 205/2017 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a zároveň byla vydána související vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti, která definuje základní povinnosti subjektů, které provozují kritickou informační infrastrukturu nebo významný informační systém.[102]

Vzhledem k současným trendům v oblasti kybernetické bezpečnosti, rychlosti, účelnosti a míře provedení kybernetických útoků a zároveň vzhledem k ceně bezpečnostních opatření je mylné se domnívat, že v této oblasti se bez přispění uživatelů i vedoucích funkcionářů něco radikálně změní. Při probíhajícím útoku je již pozdě se ptát, co jsme v oblasti bezpečnosti ICT udělali pro to, abychom zmírnili jeho dopad.

[102]ŠULC, V. *Kybernetická Bezpečnost.* Plzeň, 2018, s. 12.

Závěr

Bakalářská práce se zaměřila na kybernetickou kriminalitu v prostředí Internetu. Toto prostředí je svou různorodostí a rostoucím počtem uživatelů živnou půdou pro pachatele. Se stále se rozvíjejícími technologiemi se rozšiřují možnosti provedení útoků. Na základě nových technologií vznikají nové typy hrozeb, nebo se modifikují stávající. S rozšířením IoT se stanou ohrožené i věci, které v domácnosti budou k Internetu připojeny. Lze si jistě představit řadu scénářů, při kterých pachatel může využít domácí ledničku, kávovar, televizi apod. V budoucnu vznikne botnetová síť složená ze zařízení připojených do IoT. Kyberzločinci moc dobře vědí, že do Internetu je již nyní připojena spousta chytrých věcí, které jejich majitelé nechávají bez povšimnutí a na které neaplikují poslední aktualizace vydané výrobci (pokud takové jsou).

Cílem bakalářské práce bylo analyzování kybernetické kriminality v prostředí Internetu, druhotným cílem pak zhodnocení směrů vývoje vybraných typů kybernetické kriminality, která má za cíl finančně, nebo psychicky poškodit oběti trestné činnosti.

Analyzování kybernetické kriminality, přehledné shrnutí základních pojmů bylo provedeno v popisné části (kapitoly 2, 3, 4, 5), kde byly popsány jednotlivé formy tohoto druhu kriminality, její historie a budoucí vývoj s poukázáním na nejpoužívanější formy.

V roce 2018 pokračovaly plošné útoky vyděračským softwarem typu ransomware, které cílily na firmy a domácnosti. Byly zaznamenány útoky organizovaného zločinu a spojení klasické kriminality s počítačovou. Na Internetu už kybernetické zločince nezajímá jen poškození obětí, nebo sláva. Jejich zaměření směřuje k zefektivnění činnosti, zjednodušení útoků a plošnému užití. Do popředí se dostávají placené služby a možnost objednat si kybernetickou kriminalitu na klíč. Změna směřování je zřejmá. Dnes jsou útoky mířeny i na kritickou infrastrukturu a její vyřazení nebo napáchání co největších škod. Tyto faktory spolu s neznalostí, arogancí a nezájmem uživatelů o bezpečnost ICT způsobují celosvětově obrovské ztráty a zařazují kybernetickou kriminalitu do popředí zájmu.

Kyberzločinci v prostředí Internetu se budou neustále vyvíjet a zlepšovat své znalosti i dovednosti. Už dnes to nejsou pouze jednotlivci. Začínají se tvořit skupiny, které se zaměřují na co největší zefektivnění a znásobení zisku. Největší zisky generuje ransomware. Do popředí se začínají dostávat i programy, které mimo pozornost

uživatele dokáží využít strojový čas a výkon technického prostředku k těžbě kryptoměn. Internetový zločin se jejich pachatelům vyplácí a rok od roku generuje větší a větší zisky. Odhady škod pro rok 2019 celosvětově převýší bilion dolarů.

Teoretická část práce je založena na analýze případů kybernetické kriminality, která se zaměřila na finanční a psychické škody působené obětím. Dále byla v teoretické části shrnuta fakta, jak se nárůst kybernetické kriminality promítnul do současné společnosti (kapitoly 6,7). V této části bylo zmíněné prolnutí popisné a teoretické části práce nejvíce znatelné. Obě části jsou spolu velmi úzce propojeny.

V poslední kapitole práce se autor zaměřil na zhodnocení nárůstu kyberkriminality a její promítnutí do společnosti včetně vývoje bezpečnosti v České republice.

Autor práce má za to, že pro potřeby práce bylo nejdříve třeba vysvětlit pojmy kybernetické kriminality. Při psaní se autor neustále opíral o myšlenku, že největší díl bezpečnosti leží především na uživateli. Dle názoru autora práce je provedení prevence a osvěty ze strany odborné veřejnosti, škol a jiných institucí nutností k vedení účinné obrany. Bylo by velmi žádoucí, aby počet odborníků v ICT vzrůstal a více se do problematiky zapojovala i laická veřejnost a média. Vzrůst by měl také počet odborníků v oblasti bezpečnosti a ochrany kritické infrastruktury státu.

Motivací autora, při vybírání tématu bakalářské práce byla snaha alespoň malým dílkem přispět k tomu, aby se o potírání kybernetické kriminality v prostředí Internetu a nebezpečí z ní plynoucí více rozšířilo do povědomí běžných uživatelů.

Kybernetická kriminalita je fenoménem doby, zločincům se vyplácí a generuje větší zisky než obchod s drogami. Jedinci, firmy i státy se dnes prostřednictvím počítačových sítí a různých technických prostředků čím dál více stávají součástí kyberprostoru a tedy i potencionálním cílem pachatelů kybernetické kriminality. Dalším mimořádně nebezpečným jevem je lidský faktor. Je potřeba aktivně se zapojit do osvěty veřejnosti v oblasti používání informačních technologií a jejich možných úskalí. Dále pak je třeba se zapojit do výchovy odborníků, kteří se budou podílet na potírání kybernetických zločinů. Hrozbám z Internetu se lze do jisté míry bránit hlavně poučením uživatelů o nástrahách chování na Internetu a z něj plynoucích nebezpečí. Také plně zabezpečený a neustále aktualizovaný počítač, mobilní telefon nebo jiný technický prostředek je základem k odrazení pachatele od jeho úmyslů. Pokud nepůjde

o cíleně zaměřený útok, je pro pachatele vždy jednodušší vybrat si cestu nejmenšího odporu.

Seznam použitých zdrojů

Literární zdroje

1. KOLOUCH, J. *Cybercrime*. Praha : CZ.NIC, 2016. 522 s. ISBN 978-80-88168-15-7.
2. SMEJKAL, V. *Kybernetická kriminalita.* Plzeň : Aleš Čeněk, 2018. 934 s. ISBN 978-80-7380-720-7.
3. JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti*. Praha : Policejní akademie, 2013. 200 s. ISBN 978-80-7251-379-0.
4. SMEJKAL, V., VLČEK, M., SOKOL, T. *Počítačové právo*. Praha : Beck/SEVT, 1995. 264 s. ISBN 80-7179-009-5.
5. YONAZI, J. J., SEDOYEKA, E., ARIWA, E., EL-QAWASMEH, E. *e-Technologies and Networks for Development.* Heidelberg : Springer, 2011. 366 s. ISBN 978-3-642-22729-5.
6. MUSIL, S. *Počítačová kriminalita*. *Nástin problematiky*. Praha : Kufr, 2000. 299 s. ISBN 80-86008-80-0.
7. KOŽÍŠEK, M., PÍSECKÝ V. *Bezpečně na internetu. Průvodce chováním ve světě online*. Praha : Grada Publishing, 2016. 176 s. ISBN 978-80-247-5595-3.
8. MEYER-SCHÖNBERGER, V., CUKIER, K. *Big Data.* Brno : Computer Press, 2014. 256 s. ISBN 978-80-251-4119-9.
9. KRÁL, M. *Bezpečný internet. Chraňte sebe i svůj počítač.* Praha : Grada Publishing, 2015. 184 s. ISBN 978-80-247-5453-6.
10. ŠULC, V. *Kybernetická Bezpečnost.* Plzeň : Aleš Čeněk, 2018. 148 s. ISBN 978-80-7380-737-5.
11. ROGERS, V. *Kyberšikana. Pracovní materiály pro učitele a žáky i studenty.* Praha : Portál, 2011. 104 s. ISBN 978-80-7367-984-2.
12. MCCARTHY, L., WELDON-SIVIY, D. *Bud pánem svého prostoru. Jak chránit sebe a své věci, když jste online*. Praha : CZ.NIC, 2013. 316 s. ISBN 978-80-904248-6-9.

Elektronické zdroje

1. *Podíl domácností s internetem stoupl na 80 %, ČR zaostává za EU* [online]. 2019 [cit. 2018-11-23]. Dostupné z WWW: <https://www.ceskenoviny.cz/zpravy/podil-domacnosti-s-internetem-stoupl-na-80-cr-zaostava-za-eu/1688960>.

2. *Cracker* [online]. San Francisco (CA) : Wikimedia Foundation, 2001 [cit. 2018-11-04]. Dostupné z WWW: <https://cs.wikipedia.org/wiki/Cracker>.
3. *Cyberspace* [online]. Sharpened Productions, 2019 [cit. 2018-11-04]. Dostupné z WWW: <https://techterms.com/definition/cyberspace>.
4. *Dark Web – The Unexplored Cyberspace* [online]. San Francisco (CA) : Medium.com, 2018 [cit. 2019-02-22]. Dostupné z WWW: <https://medium.com/coinmonks/dark-web-the-unexplored-cyberspace-5009ca0ecd87>.
5. FIALOVÁ, R. *Počítačová kriminalita v České republice* [online]. Brno : Masarykova univerzita, 2001 [cit. 2018-12-05]. Dostupné z WWW: <ttps://www.fi.muni.cz/usr/jkucera/pv109/2001/xfialov1.html>.
6. *INTERNET USAGE STATISTICS. The Internet Big Picture* [online]. Bhópál : Miniwatts Marketing Group, 2018 [cit. 2018-12-30]. Dostupné z WWW: <www.internetworldstats.com/stats.htm>.
7. *Internet* [online]. San Francisco (CA) : Wikimedia Foundation, 2001 [cit. 2018-12-14]. Dostupné z WWW: <https://wikipedia.org/wiki/Internet>.
8. *Adware: Definition and Removal Guide* [online]. Copenhagen : hemdalsecurity.com, 2017 [cit. 2019-01-13]. Dostupné z WWW: <https://heimdalsecurity.com/blog/adware-definition-removal>.
9. *What is a Keylogger?* [online]. Moskva : Kaspersky, 2019 [cit. 2019-01-13]. Dostupné z WWW: <https://www.kaspersky.com/resource-center/definitions/keylogger>.
10. *What is Ransomware?* [online]. Moskva : Kaspersky, 2019 [cit. 2019-01-13]. Dostupné z WWW: <https://www.kaspersky.com/resource-center/definitions/what-is-ransomware>.
11. *Easy, Cheap, and Costly: Ransomware is Growing Exponentially* [online]. San Jose (CA) : umbrella.cisco.com, 2015 [cit. 2019-01-13]. Dostupné z WWW: <https://umbrella.cisco.com/blog/2015/09/02/easy-cheap-and-costly-ransomware-is-growing-exponentially>.
12. *What is a Scareware?* [online]. Moskva : Kaspersky, 2019 [cit. 2019-01-13]. Dostupné z WWW: <https://www.kaspersky.com/resource-center/definitions/scareware>.
13. *The ultimate guide to scareware protection* [online]. New York : ZDNet, 2009 [cit. 2019-01-13]. Dostupné z WWW: < https://www.zdnet.com/article/the-ultimate-guide-to-scareware-protection/>.

14. *What is a Spyware? - Definition* [online]. Moskva : Kaspersky, 2019 [cit. 2019-01-13]. Dostupné z WWW: < https://www.kaspersky.com/resource-center/threats/spyware>.
15. *What is a Computer Virus or a Computer Worm?* [online]. Moskva : Kaspersky, 2019 [cit. 2019-01-13]. Dostupné z WWW: <https://www.kaspersky.com/resource-center/threats/viruses-worms>.
16. *Antivirové kukátko: dnes Avast!* [online]. Praha : Zive.cz, 2005 [cit. 2019-01-13]. Dostupné z WWW: < https://www.zive.cz/clanky/antivirove-kukatko-dnes-avast/sc-3-a-122212/default.aspx>.
17. *What is a Computer Virus or a Computer Worm?* [online]. Moskva : Kaspersky, 2019 [cit. 2019-01-13]. Dostupné z WWW: <https://www.kaspersky.com/resource-center/threats/viruses-worms>.
18. *Drive-by Downloads* [online]. Australia : Australian Government, 2012 [cit. 2018-12-01]. Dostupné z WWW: <https://acsc.gov.au/publications/protect/Drive-by-Downloads.pdf>.
19. EUROPOL. *IOCTA: Internet Organised Crime Threat Assessment* [online]. Europol : European Cybercrime Centre, 2018 [cit. 2019-01-20]. Dostupné z WWW: <www.europol.europa.eu>.
20. NOVÁK, M., Chripák, D. *Grafika: Strach z Huaweie. Západ burcuje kvůli špionáži, Čína vyrazila do protiútoku* [online]. Praha : Aktuálně.cz, 2019 [cit. 2019-03-01]. Dostupné z WWW: <http://zpravy.aktualne.cz/zahranici/huawei-prehledne-o-sporu/r~6464075a26011e996370cc47ab5f122>.
21. *Blokchain* [online]. San Francisco (CA) : Wikimedia Foundation, 2001 [cit. 2019-01-14]. Dostupné z WWW: < https://cs.wikipedia.org/wiki/Blockchain >.
22. *Big data. Nové způsoby zpracování a analýzy velkých objemů dat.* [online]. Praha : CCB, 2011[cit. 2018-12.12]. Dostupné z WWW: <https://www.systemonline.cz/clanky/big-data.htm>.
23. PIKORA, A. *Umělá inteligence ve službách útočníků.* [online]. Praha : Nitmedia, 2018 [cit. 2018-12-14]. Dostupné z WWW: < https://www.itbiz.cz/clanky/umela-inteligence-ve-sluzbach-utocniku>.
24. *Stinná stránka umělé inteligence, stroje pomáhají kyberzločincům* [online]. Cambridge : Novinky.cz, 2018 [cit. 2018-12-30]. Dostupné z WWW:

<https://www.novinky.cz/internet-a-pc/bezpecnost/464210-stinna-stranka-umele-inteligence-stroje-pomahaji-kyberzlocincum.html>.

25. *BUCNOST FAKE NEWS: Deep fake videa* [online]. Praha : Manipulátoři.cz, 2019 [cit. 2019-02-20]. Dostupné z WWW: <https://manipulatori.cz/budoucnost-fake-news-deep-fake-videa/>.
26. TOPINKOVÁ, M. *Policie varuje před počítačovým virem, který se šíří internetem v Česku* [online]. Praha : iDnes.cz, 2012 [cit. 2018-12-10]. Dostupné z WWW: <https://www.idnes.cz/zpravy/cerna-kronika/sireni-pocitacoveho-viru.A121008_144459_domaci_maq>.
27. *Ransomware – „policejní virus" na pitevním stole* [online]. Praha : ROOT.CZ, 2013 [cit. 2018-12-11]. Dostupné z WWW: <https://www.root.cz/clanky/ransomware-policejni-virus-na-pitevnim-stole/>.
28. *WannaCry a Petya způsobily škody za více než 4 miliardy dolarů* [online]. Praha : ROOT.CZ, 2017 [cit. 2019-01-11]. Dostupné z WWW: <https://www.root.cz/zpravicky/wannacry-a-petya-zpusobily-skody-za-vice-nez-4-miliardy-dolaru/>.
29. *WannaCry* [online]. Redwood City (CA) : AVAST.COM, [cit. 2019-02-01]. Dostupné z WWW: < https://www.avast.com/cs-cz/c-wannacry>.
30. *Ransomware je na vzestupu, vydírání si můžete objednat* [online]. Praha : ROOT.CZ, 2017 [cit. 2019-02-01]. Dostupné z WWW: <https://www.root.cz/clanky/ransomware-je-na-vzestupu-uz-laka-i-amaterske-kyberzlocince/>.
31. *Executive Summary. 2018 Internet Security Threat Report* [online]. Mountain View : Symantec, 2018 [cit. 2019-02.02]. Dostupné z WWW: <https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf>.
32. *Hledám kluka z autobusu* [online]. Praha : Zpovědnice, 2014 [cit. 2019-02-27]. Dostupné z WWW: <https://www.zpovednice.cz/detail.php?statusik=824724>.
33. *Kyberšikana* [online]. Olomouc : Centrum PRVoK PdF UP, 2010 [cit. 2019-03-01]. Dostupné z WWW: <https://www.e-bezpeci.cz>.
34. *Kyberkriminalita* [online]. Praha : Policie ČR, 2019 [cit. 2019-02-22]. Dostupné z WWW: <www.policie.cz/clanek/kyberkriminalita.aspx>.

Legislativní dokumenty

1. ČESKO. Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In Sbírka zákonů, Česká republika. 2014, částka 75, s. 1926-1936.

Ostatní zdroje

Kromě výše uvedených zdrojů byly při zpracování bakalářské práce využity následující materiály:

- TV pořad Fokus Václava Moravce ze dne 12. prosince 2017.

Seznam zkratek

AI (Artificial Intelligence) – Umělá inteligence

ARPANET (Advanced Research Projects Agency Network) – grantová agentura ministerstva USA, počítačová síť, předchůdce současného Internetu.

C&C (Control and Command) – Řídící server Botnetu

ČVUT – České vysoké učení technické v Praze

DDoS (Distributed DoS) – podtyp útoku typu DoS

DoS (Denial of Service) – odepření služby

DRDoS (Distributed Reflection DoS) – podtyp útoku DoS

PC (Personal Computer) – osobní počítač.

SMEP – Systém malých elektronických počítačů

TCP/IP (Transmission Control Protocol/Internet Protocol) – Primární přenosový protokol/protokol síťové vrstvy

ICT (Information and Communication Technologies) – Informační a komunikační technologie

IOCTA (Internet Organised Crime Threat Assessment) – Výroční zpráva Europolu o růstu a průběhu kybernetické kriminality

IoT (Internet of Things) – Internet věcí

IP (Internet Protocol) – Jednoznačný identifikátor síťového rozhraní technického prostředku

IT – Informační technologie

KGB – Výbor státní bezpečnosti, sovětská tajná služba

LEO (Lyons Electronics Office) – první počítač určený ke komerčnímu využití

NSFNET (National Science Foundation Network) – síť, která propojovala výkonné počítače v USA, předchůdce Internetu

OČTŘ – Orgány činné v trestním řízení

WWW (World Wide Web) – celosvětová síť

Seznam tabulek a grafů