POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně právní

Katedra kriminologie

Kyberkriminalita – kriminologické aspekty

Bakalářská práce

Cybercrime - criminological aspects

Bachelor thesis

VEDOUCÍ PRÁCE
Mgr. Najman Tomáš

AUTOR PRÁCE
Šimon Katz

PRAHA
2022

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Praze, dne ……

.....

Šimon Katz

Anotace

Bakalářská práce na téma „Kyberkriminalita – kriminologické aspekty“ pojednává o problému kriminality spojené s užíváním informačních technologií. V prvních dvou kapitolách je definována především základní terminologie související s informačními technologiemi a definice pojmů relevantních pro tuto práci. Následující kapitoly se věnují konkrétním typům útoků v rámci kyberprostoru. V závěru práce jsou popsány možné stupně ochrany a prevence před danými útoky, a následně vybrány některé legislativní předpisy sloužící k ochraně proti a případné represi za trestné činy na území České republiky.

Klíčová slova

Počítač, kyberprostor, kybernetický útok, kybernetická kriminalita, hacking, prevence,

Annotation

The bachelor thesis on "Cybercrime – Criminological Aspects" deals with the problem of crime related to the use of information technology. In the first two chapters, the basic terminology related to information technology and the definition of terms relevant to this thesis is defined. The following chapters deal with specific types of attacks within cyberspace. The thesis concludes with a description of the possible levels of protection and prevention against these attacks, followed by a selection of some legislative provisions serving to protect againt cybercrime and possibly repress criminal offences in the Czech Republic.

Keywords

Computer, cyberspace, cyber attack, cybercrime, hacking, prevention

Obsah

Úvod

V návaznosti na současný vývoj informačních technologií a společnosti je všeobecně akceptováno, že se počítače, mobilní zařízení a jiná elektronická zařízení připojená do globální sítě staly téměř neodmyslitelnou součástí našich životů a pronikají nám jak do pracovního, tak i osobního prostředí. Tento fenomén není obecně vnímán jako negativní, musí se však počítat s tím, že s rapidním vývojem technologií se také zvyšují rizika a hrozby s technologiemi spojené.

Tento vývoj informačních technologií má za následek zvýšení kvality a rychlosti přenosu informací, s tím však vzniká nutnost zaměřit se i na ochranu těchto potencionálně důležitých a kritických informací. Negativním aspektem tohoto prudkého technologického pokroku je nárůst tzv. *Kybernetické kriminality*. Útočníci neustále vymýšlejí a nacházejí nové a zároveň sofistikovanější způsoby, jak proniknout do chráněných systémů, velice rychle se adaptují na aktuální trendy ve snaze informace změnit, zničit, ukrást nebo jinak zneužít pro svůj prospěch nebo ve prospěch jiných osob či organizací.

Kybernetická kriminalita je momentálně problematičtější, než by se mohlo běžnému člověku na první pohled zdát. Téměř každý byl vystaven nějaké formě kybernetické kriminality nebo pokus o ní. Jelikož je v posledních letech častěji než kdykoliv předtím využíváno informačních technologií k páchání trestné činnosti jak jednotlivými pachateli, tak kriminálními a teroristickými organizacemi, tak dochází k zvýšení nebezpečnosti napadení běžného uživatele či kritických infrastruktur společností a státu.

Proto se současně s kriminalitou rozvíjí také informační bezpečnost jako praktický obor, jenž má na starost ochranu informací jak osob fyzických, tak právnických. Primárně se zabývají tyto obory preventivní stránkou ochrany, aby nedošlo ke ztrátě integrity, důvěrnosti a případné dostupnosti informací. V rámci represe je důležitá legislativa, díky které je možné efektivně potrestat pachatele kyberkriminality.

Cíl práce

Cílem práce je popis fenoménu kybernetické kriminality, jeho rozbor, specifika a popis jednotlivých aktérů. V práci jsou uvedené základní definice související s kybernetickou kriminalitou, vysvětleny jednotlivé typy kybernetických útoků, a zároveň jejich případná prevence z hlediska osobní ochrany a technického zabezpečení. V rovině represe jsou zmíněny legislativní opatření spojené s tímto fenoménem, a to jak v České republice, tak na úrovni mezinárodní. Ke konci práce je zhodnocení dosavadního statistického reportu kybernetické kriminality od Policie ČR.

1. Vymezení základních pojmů

1.1. Počítač

Každý počítač se skládá z různých fyzických tedy hardwarových a programových tedy softwarových komponent, které pak můžeme náležitě rozdělit podle jejich funkce využití například počítač osobní to je notebook a stolní počítač nebo server či disková pole atd.[1]

1.1.1. Hardware

Každý počítač je složen z několika základních částí. Procesor, grafická karta, operační paměti, zvuková karta, pevné disky k ukládání dat, a to vše je připojeno na základní desce známé taky jako motherboard a vše je napájeno zdrojem. Dále pak k mohou být k počítači připojeny vstupní a výstupní periferie těmi rozumíme věci jako sluchátka, klávesnice, myš, tiskárna, scanner atd.[1]

1.1.2. Software

Druhou součástí počítače je již zmíněné programové vybavení, které vzniká tvořivou činností autora. Software lze definovat jako jakýsi soubor instrukcí dat, anebo programů, které jsou nutné k ovládání počítače a jiných požadovaných úkolů. Software je tedy široký pojem zahrnující, kterým označujeme aplikace a programy spustitelné na počítači. Zatímco hardware počítače je statická část počítače software je dynamický a stále se měnící součástí. [2]

Softwarový program je chráněn je autorským právem podle zákona č. 121/2000 Sb., Zákon o právu autorském, §2 odst. 2. ve znění *„Za dílo se považuje též počítačový program, fotografie a výtvor vyjádřený postupem podobným fotografii, které jsou původní v tom smyslu, že jsou autorovým vlastním duševním výtvorem. Databáze, která je způsobem výběru nebo uspořádáním obsahu autorovým vlastním duševním výtvorem a jejíž součásti jsou systematicky nebo metodicky uspořádány a jednotlivě zpřístupněny elektronicky či jiným způsobem,*

---

[1] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. Pro praxi. ISBN 978-80-7380-501-2.

[2] ROSENCRANCE, Linda. *Software* [online]. [cit. 2022-07-12]. Dostupné z: https://www.techtarget.com/searchapparchitecture/definition/software

je dílem souborným. Jiná kritéria pro stanovení způsobilosti počítačového programu a databáze k ochraně se neuplatňují.“ [3]

Avšak i přesto, že zákon v několika instancích pracuje ze slovy „počítačový program“ nebo „software“ žádný ze zákonů jej nijak blíže nedefinuje než jako autorské dílo podle §2 odst. 1 zákona č.121/2000 Sb., Zákon o autorském právu, ve znění „*Předmětem práva autorského je dílo literární a jiné dílo umělecké a dílo vědecké, které je jedinečným výsledkem tvůrčí činnosti autora a je vyjádřeno v jakékoli objektivně vnímatelné podobě včetně* ***podoby elektronické****, trvale nebo dočasně, bez ohledu na jeho rozsah, účel nebo význam.“* [4]

1.2. Kyberprostor

V české legislativě je kyberprostor definován v zákoně č.181/2014 Sb. „Zákon o kybernetické bezpečnosti“ pod §2 písmenem a) „*kybernetickým prostorem digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací*“.[5]

Kyberprostor je možno definovat jako virtuální místo v internetové síti na niž je závislý, neboť i přesto že lze kyberprostor téměř bezmezně zvětšovat, zmenšovat, přizpůsobovat našim požadavkům dojde-li k zániku technologie internetu zanikne i veškerý kyberprostor. Kyberprostor jako takový je pak tvořen interakcí s informačními a komunikačními technologiemi.

Hlavními znaky kyberprostoru jsou globalita, volný přístup pro téměř jakéhokoliv uživatele, rychlost a možnost vyhledávání v až může se zdát nekonečných informacích, avšak s tolika informacemi přichází problém s výskytem nepravdivých a zkreslených informací.

---

[3] *Zákon o právu autorském* [online]. [cit. 2022-20-02]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-121

[4] *Zákon o právu autorském* [online]. [cit. 2022-20-02]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-121

[5] *Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů* [online]. [cit. 2022-15-02]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

Kyberprostor je rozdělen na tři vrstvy, které nejsou fyzicky nijak odděleny, ale jsou přístupné za jiných podmínek.

První vrstvou je takzvaný Surface web. Jedná se o část internetu, která je plně dostupná většině uživatelů, kteří s ním mohou interagovat a využívat jej v zásadě bez jakýchkoliv jiných podmínek, kromě přístupu k samotnému internetu a internetový prohlížeč. Tato část kyberprostoru obsahuje stránky jako Google, YouTube, Bing, Wikipedia aj.

Druhou vrstvou je Deep web. Toto je část internetu, která většinou vyžaduje jakési přihlášení nebo přistup do soukromé sítě (například firemní intranet). Po přihlášení se nám „odemkne“ obsah dané stránky. Například se může jednat o sítě internetového bankovnictví, cloudová úložiště, sociální sítě, emailové schránky atd. zkrátka vše co bez přihlášení nelze vidět.

Třetí vrstvou je Dark web. Na to, aby se běžný uživatel dostal na stránky, které jsou umístěny na Dark webu tak potřebuje povětšinou anonymní prohlížeč a konkrétní adresy (peer-to-peer připojení) nebo přítele který je na konkrétní stránce připojen (tzv. Friend-to-friend připojení). Na Dark Webu se lze dostat k utajovaným informacím, nájemným vraždám, dětské pornografii, prodej a nákup drog, falšovaných nebo kradených občanských a řidičských průkazů či pasů, kreditní karty nebo zbraně. Jedním z nejznámějších takovýchto nelegálních tržišť byl „Silk Road“, anebo stále ještě je „The Armory“ na kterém dochází k obchodu s nelegálními zbraněmi.[6]

1.3. Kybernetický útok

Kybernetický útok lze definovat jako jakákoliv protiprávní jednaní, které je vykonáno v kyberprostoru a má za cíl uškodit jiné osobě, přičemž se nemusí nutně jednat o činnost trestnou. Spoustu druhů kybernetické kriminality lze přiřadit pod konkrétní právní normy trestního zákoníku, avšak najdou se i takové které je velice obtížné zařadit nebo vůbec definovat. Kybernetickým útokem může být útok jak v kyberprostoru, tak i útok na hardwarová zařízení.[7]

---

[6] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. s. 42-54. ISBN 978-80-88168-15-7.
[7] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. s. 54-56. ISBN 978-80-88168-15-7.

2. Kyberkriminalita

„Kyberkriminalita neboli informační kriminalita, je nejdynamičtějším typem kriminality současnosti a kybernetické incidenty patří dnes mezi nejzávažnější hrozby pro společnost ve vyspělých zemích. Při značném zjednodušení se kyberkriminalitou rozumí ty formy kriminality, které jako nástroj využívají nebo jako cíl směřují na moderní informační a komunikační technologie. Prioritami v potírání kyberkriminality v České republice je v současné době zejména boj proti dětské pornografii, majetkové trestné činnosti na internetu, porušování autorských práv, aktivitám směřujícím k vylákání zneužitelných osobních údajů“ [8]

2.1. Specifika kyberkriminality

2.1.1. Nízké náklady a dostupnost

V dnešní době je kyberprostor téměř všudy přítomným existujícím nezávisle na vůli jednotlivce a připojení do něj nebylo nikdy snazší a neustávající vývoj informačních technologií způsobil téměř nutnost vlastnit nějaké chytré zařízení. Počítač, chytrý telefon, chytré hodinky atd. jsou dnes poměrně levnou a dostupnou záležitostí, a i přes to, že jejich primární účel nikdy nebyl trestná činnost tak jejich neblahým vedlejším účinkem je její poměrné usnadnění. Právě nízké náklady a dostupnost těchto zařízení dělá kyberkriminalitu tak lákavou, neboť pachatel potřebuje pouze sadu dovedností, vybavení a připojení k síti, které je skoro všudy přítomné.[9]

2.1.2. Globálnost

Dalším specifikem je globálnost kybernetické kriminality, neboť právě globálnost kyberprostoru a internetu dává pachatelům možnost útočit na oběti nacházející se prakticky kdekoliv na planetě bez nutnosti vlastního fyzického kontaktu s obětí. Globálnost také ztěžuje odhalování a dokazování většiny trestné činnosti v kyberprostoru právě kvůli možnosti útoků kamkoliv mimo státní hranice.

---

[8] Policie ČR: *Hlášení kyberkriminality* [online]. [cit. 2022-06-09]. Dostupné z: https://www.policie.cz/clanek/hlaseni-kyberkriminality.aspx

[9] MARAS, Marie-Helen. Cybercriminology. New York;Oxford; Oxford University Press, 2017. s. 3-5. ISBN 978-01-90278-44-1;

„V současnosti je většina kyberkriminality spojena s internetem, ale bez významu
nejsou ani další sítě (např. uzavřená firemní síť bez připojení na internet, síť řídící procesy v elektrárně atp.). Jedná se o otevřený systém bez jediného řídícího centra, naopak drtivá většina aktivit (např. zobrazení webové stránky) probíhá vždy prostřednictvím několika serverů. Přenos dat mezi zařízeními tak mnohdy prochází přes různé státy, i když se obě zařízení nachází na stejném místě. Je proto mnohdy nejasné, ve které zemi jsou uložena data a přes které státy byla transportována. Globálnost kyberprostoru vede tedy často také k problematickému postihu prostřednictvím tradičního trestního systému založeného na státní suverenitě.“[10]

2.1.3. Anonymita

Atraktivní je pro pachatele také anonymita kyberprostoru, kde lze používat falešná jména či fotografie, tento fakt pak dává pachatelů pocit anonymity, která je ve skutečnosti zdánlivá, neboť pachatel za sebou může nechat vypátratelné digitální stopy. Právě pocit anonymity a neodhalitelnosti často dodává pachatelům odvahu trestnou činnost páchat.[11]

2.1.3.1. Digitální stopy

V návaznosti na anonymitu internetu je důležité vysvětlit, proč je zdánlivá, a co jsou to vlastně ony zmíněné digitální stopy.

Digitální stopy lze rozdělit podle toho, zdali je možné je chováním uživatele do jisté míry ovlivnit či nikoliv, a to na tzv. digitální stopy neovlivnitelné a digitální stopy ovlivnitelné.

a) Digitální stopy neovlivnitelné

Neovlivnitelnost těchto stop není absolutní, nicméně jakákoliv manipulace s nimi (jako např. změna, skrytí, nebo jejich potlačení) je složitější, neboť vyžaduje více než standardní znalosti této problematiky. Tyto stopy vznikají v zásadě jakoukoliv interakcí dvou počítačových systémů mezi sebou, anebo fungováním

[10] GŘIVNA, Tomáš, SCHEINOST, Miroslav a ZOUBKOVÁ, Ivana. *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. s. 390. ISBN 978-80-7598-554-5.
[11] GŘIVNA, Tomáš, SCHEINOST, Miroslav a ZOUBKOVÁ, Ivana. *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. s. 392. ISBN 978-80-7598-554-5.

systému samotného. Obecně jsou tyto stopy například ve formě chybových logů operačního systému, informací o systému samotném nebo informací uložených poskytovatelem nejrůznějších služeb na internetu (návštěvnost, délka návštěvy na stránce, co uživatel vyhledával apod).

Konkrétním příkladem takové stopy je **IP adresa**. Velice zjednodušeně má každý počítačový systém svou IP adresu, kterou jednotlivá zařízení potřebují k možnosti komunikace s jinými systémy. IP adresa pak takovému systému slouží jako jeden z identifikátorů zařízení, se kterým právě komunikuje. *„Díky přísným pravidlům definujícím hospodařeni s IP adresami a veřejně přístupnými databázemi, RIR (Regional Internet Registry), které obsahuji informace o držitelích jednotlivých adresových bloků, je možné velmi rychle zjistit, do které sítě patři určitá IP adresa a kdo danou síť provozuje. Provozovatel dané sítě pak díky logovaní informaci ze síťového provozu dokáže identifikovat, kdo (respektive jaký počítačový systém) v konkrétním čase používal konkrétní IP adresu. Toto určeni je velmi důležitým zdrojem informaci při řešeni bezpečnostních incidentů (kybernetických útoků) a při pátraní jejich po zdroji (původci).“* [12] Tomuto způsobu identifikace napomáhá fakt, že IP adresy nejsou standardně anonymní. Pokud se někdo nesnaží svou přítomnost záměrně utajit, je poměrně nenáročné takového uživatele vypátrat.

Další stopou je obyčejný email. Emailová zpráva má ve zdrojovém kódu uloženo velké množství informací. Mezi ně bývá řazen například název počítače a jeho operační systém, čas odeslání zprávy, jméno poskytovatele služby a serverovou cestu. Díky IP adrese pak taková informace zahrnuje i skutečného odesílatele, odesílal-li emailovou zprávu z nově vytvořeného falešného profilu.

V neposlední řadě všelijaké stopy uchovává samotný webový prohlížeč. Ten standardně předává informace o uživateli a jeho systému navštíveným

[12] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. s. 138. ISBN 978-80-88168-15-7.

stránkám. Například odkud se uživatel na konkrétní webovou stránku dostal, jaký používá prohlížeč atd. [13]

b) Digitální stopy ovlivnitelné

Touto stopou je jakékoliv informace, kterou uživatel vědomě a dobrovolně sám poskytne jiné osobě, ať už fyzické či právnické. Poskytnutím si můžeme představit odesílání emailových zpráv, konverzace na instantních messengerech (Whatsapp, Facebook aj.), příspěvky do diskusí, ale i zveřejňování médií jako jsou fotografie a videa na sociálních sítích. Do těchto stop patří mimo jiné registrace v rámci soukromých sítí a jejich další využívání. Takových služeb je v kyberprostoru nepřeberné množství, mohou to být cloudová úložiště, P2P a F2F sítě, chatovací služby, sociální sítě atd.

Jde tedy o stopy, které jsou primárně ovlivněny tím, co o sobě uživatel sdílet chce a co ne. [14]

V rámci digitálních stop je důležité mít na paměti, že: „*Ve světě ICT platí jedno pravidlo: pokud kdykoliv cokoliv nahrajete, přenesete, zprostředkujete, vložíte do kyberprostoru, zůstane to tam „navždy“. Vždy bude existovat kopie (vznikla na základě funkcionality počítačového systému či kopie uložena některým jiným uživatelem) vašich dat. A i když tato data následně odstraníte (či je odstraní někdo jiny), k jejich skutečnému, trvalému a nezvratnému odstraněni nedojde. Je proto vhodné věnovat pozornost své digitální stopě a informacím či datům, jež za sebou v prostředí kyberprostoru zanecháváme.“* [15]

2.1.4. Latence

Oblast kybernetické kriminality se potýká se značnou latencí tedy nevíme, jak velký rozsah kyberkriminalita vlastně má. Latence je často spojena s tím, že oběť ani neví, že se stala cílem útoku kvůli neodhalení hrozby na svém zařízení, popřípadě neví, že je dané jednání trestné, tudíž jej neohlásí. Faktorem pro vysokou latenci kyberkriminality oproti tradiční kriminality je také neviditelnost

---

[13] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. s. 74 a 134-144. ISBN 978-80-88168-15-7.

[14] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. s. a 144-145. ISBN 978-80-88168-15-7.

[15] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. s. 135 a 134-148. ISBN 978-80-88168-15-7.

následků útoku. Anebo nevědomost pachatelů, že páchají trestnou činnosti či naopak uvědomění si, že trestnou činnost páchají, a to je odrazuje od jejího nahlášení.[16]

2.2. Pachatel

Nejčastěji používaný výraz pro pachatele kybernetické kriminality je pojem „hacker“. Pojmem ***hacker*** rozumíme specialistu na počítače či programátora s velice rozsáhlými znalostmi systému a se znalostmi obcházení bezpečnostních systémů. Tyto znalosti dokáže využívat k tomu, aby systém, využil nebo změnil ke svým vlastním potřebám ať už legálním nebo nelegálním. Hackerem může být kdokoliv ve našem okolí, avšak ne všichni hackeři mají primárně nekalé úmysly. Původně nebyl však pojem hacker nebyl vnímán jako negativní, výraz byl vymyšlen studeny Massachusetts Institute of Technology, kteří pracovali na jednom z prvních počítačů vůbec *„z počátku nevedlo k negativním konotacím, ani destruktivním či vandalským činnostem. Při budování sítí šlo o běžný a žádoucí přístup části skupin, které se zabývaly programováním.“* Avšak v dnešní době již bude v mainstreamových mediích pravděpodobně slovo hacker používáno ve zprávách o kybernetické kriminalitě. [17]

Typy pachatelů kybernetické kriminality nelze konkrétně charakterizovat: „*Z hlediska charakteristiky pachatele záleží vždy na druhu či typu trestné činnosti, které se dopouští, neexistuje typický pachatel kyberkriminality, předpokladem je pouze základní uživatelská znalost kyberprostoru*“[18]

2.2.1. Hacking

Hacking jako takový není nelegální činností do té doby, než začne hacker ohrožovat či zneužívat systém a informace bez vědomí jejich vlastníka.

---

[16] GŘIVNA, Tomáš, SCHEINOST, Miroslav a ZOUBKOVÁ, Ivana. *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. s. 391. ISBN 978-80-7598-554-5.
[17] ZAVRŠNIK, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7552-758-5.
[18] GŘIVNA, Tomáš, SCHEINOST, Miroslav a ZOUBKOVÁ, Ivana. *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. s. 392. ISBN 978-80-7598-554-5.

Podle typů útoků můžeme hackery rozlišit na amatérské a profesionální hackery v návaznosti na to jakou znalost technologií konkrétní útoky vyžadují. [19]

Dále bychom pak mohli hackery rozřadit do kategorií podle jejich motivací.

2.2.1.1. Black Hats

Hackeři, kteří mají velice rozsáhlé znalosti o tom, jak se dostat do počítačů počítačových sítí a přes bezpečností prvky a protokoly. K tomu, aby pronikli do těchto systémů nebo je obešli, tito hackeři vytvářejí takzvaný ***malware*** (z anglického *malicious software* – škodlivý software), který jim to umožňuje.

Povětšinou bývá cílem těchto hackerů osobní nebo peněžitý zisk, avšak mohli bychom tyto hackery najít i v kontrarozvědných službách nebo teroristických organizacích kde jsou nástrojem informační a kybernetické války. Black hat hackeři nemají žádné standardy co se zkušeností týče od amatérských hackerů, kteří šíří malware jen proto, aby znepříjemňovali život, po velice dobré hackery se specifickým cílem, kterým může být krádež, záměna nebo zničení informace.

2.2.1.2. White Hats

Také známí jako „etičtí hackeři“ jsou hackeři kteří používají své schopnosti a znalosti ve prospěch druhých ve snaze je ochránit najít slabá místa systému a ty pomoci odstranit. Většinou jsou to zaměstnanci nebo externisté najmutí organizacemi jako bezpečností specialisté. White hat hackeři používají stejné metody hackování jako Black Hat hackeři s tím rozdílem, že neporušují legislativu, neboť mají svolení od organizace, která je najala, tudíž se jedná o činnost legální.

2.2.1.3. Grey Hats

Hackeři přesně na pomezí White Hats a Black Hats, nejsou to ani to. Většinou se do systému nabourají o problému organizaci informují a nabídnou, že problém za úplatu odstraní. V horším případě vaše slabé místo odhalí online, aby ho případně mohli využít jiní hackeři.

---

[19] GŘIVNA, Tomáš, SCHEINOST, Miroslav a ZOUBKOVÁ, Ivana. *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. s. 392. ISBN 978-80-7598-554-5.

Grey Hats samotní slabá místa většinou nezneužijí, ale i přesto se jedná o nelegální činnost, neboť se dostali do systému bez svolení organizace.[20]

2.2.2. Hacktivismus

Hacktivismus je velice kontroverzním pojmem které se dá spojit s různými významy, jedná se o spojení slov hacker/hacking a aktivismus. Lze definovat jako – *„použití počítačových technik, jako je hacking, jako formu občanské neposlušnosti, k propagaci politické agendy nebo společenských změn.“*[21] Většinou se setkáváme s hacktivismem, jehož primární cíl je ochránit svobodu slova, lidská práva, svobodu informací či šíření povědomí o konkrétní problematice. Nejznámější skupinou hacktivistů jsou takzvaní „Anonymous“ u kterých jak napovídá název, nikdo nezná identity jejích členů. Členové samotní se navzájem neznají a komunikují výhradě pomocí počítačových prostředků.

Hacktivismus i přestože má velice podobné znaky s kyberterorismem, terorismem být nemusí, neboť při operacích hacktivistů není primárním cílem vyvolat fyzické násilí ani způsobení permanentního poškození. Hacktivismus i přes to, že u něj pozorujeme primárně nelegální aktivity stejné jako mohou používat hackeři jde ho velice těžko lze asociovat s hackery jako takovými, neboť hacking, na rozdíl od hacktivismu, je primárně provozován za určitým ziskem či zábavou. [22]

2.3. Oběť

Avšak kromě pachatele je také vhodné zaměřit se na viktimologii tématu kybernetické kriminality. Obětí kyberútoku se může stát téměř kdokoliv, fyzická osoba, právnická osoba či jen společnost jako taková. Typická oběť stejně jako

---

[20] LASKOW, Sarah. *"The Counterintuitive History of Black Hats, White Hats, And Villains"* [online]. 2017. [cit. 2022-01-19]. Dostupné z: https://www.atlasobscura.com/articles/the-counterintuitive-history-of-black-hats-white-hats-and-villains

[21] MIKHAYLOVA, Galina. *Definice pojmu hacktivismus* [online]. 2014. [cit. 2022-01-19]. Dostupné z: https://digital.library.txstate.edu/bitstream/handle/10877/5378/MIKHAYLOVA-THESIS-2014.pdf?sequence=1

[22] Stanford University: *What is hacktivism* [online]. [cit. 2022-01-17]. Dostupné z: https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/Hacktivism/what.html

pachatel není, vždy záleží na konkrétním typu kybernetického útoku. Je několik skupin viktimizace nebo chceme-li v našem případě kyberviktimizace do kterých můžeme oběti zařadit, viktimizace primární, sekundární a terciární.

2.3.1. Primární viktimizace

V tomto případě je v rámci kybernetického útoku, útok směřován přímo proti oběti, které chce pachatel způsobit újmu. Tedy například získání přístupu na profil sociální sítě, nebo emailové schránky fyzické osoby. Anebo právnická osoba jejíž data byla ukradena.

2.3.2. Sekundární viktimizace

V rámci sekundární viktimizace je oběť v ohrožení skrze to, že pachatel se například dostal do databáze nějaké právnické osoby jako první oběti a data, která získal může nyní využít k útoku na oběť další.

2.3.3. Terciární viktimizace

Terciární viktimizace se týká dopadu kybernetické kriminality na společnost jako takovou. Například zdráhání či odmítání obětí nadále používat chytrá zařízení, či paranoia nedostatečného zabezpečení. [23]

3. Jednotlivé typy kybernetických útoků

V rámci kybernetické kriminality se můžeme setkat s poměrně širokým spektrem kybernetických útoků, které můžeme rozdělit podle Sdělení č. 104/2013

[23] MARAS, Marie-Helen. Cybercriminology. New York;Oxford; Oxford University Press, 2017. s. 3-5. ISBN 978-01-90278-44-1.

Sb. m. s. tj. Úmluva o počítačové kriminalitě do několika základních kategorií a podkategorií.[24]

a) Trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů
b) Trestné činy spočívající v šíření škodlivého obsahu
c) Trestné činy související s počítačem
d) Trestné činy spočívající v porušování práv duševního vlastnictví

3.1. Útoky proti důvěrnosti integritě a dostupnosti počítačových dat a systémů

3.1.1. Proníkání do systémů a sociální inženýrství

3.1.1.1. Phishing

Phishing je typ kybernetického útoku, který využívá manipulace a sociálního inženýrství. Cílem phishingu je uvést uživatele v omyl a to tak, že útočník rozesílá falešné emaily žádající například o ověření přístupových údajů k internetovému bankovnictví, což je také jedna z nejčastějších forem phishingu. Po odeslání těchto údajů je velice pravděpodobné že údaje již dostal pachatel, jenž tento útok zosnoval. [25] [26]

3.1.1.2. Pharming

Pharming je stejně jako phishing jedna z forem sociálního inženýrství, avšak poněkud sofistikovanější než phishing samotný. Stějně jako phishing využivá pharming lidského omylu. Uživateli přijde věrohodný e-mail od jeho banky, u kterého je buďto přiložený soubor tvářící se jako běžný formulář nebo dokument, který je ve skutečnosti pouze zamaskovaný malware a v momentě stažení tohoto falešného dokumentu máte malware v počítači. Druhou variantou je e-mail žádají dotyčného o kliknutí na odkaz tvářící se jako přihlášení do internetového bankovnictví. Kliknutím na přiložený odkaz mohou nastat dva případy. Buďto se

---

[24] GŘIVNA, Tomáš, SCHEINOST, Miroslav a ZOUBKOVÁ, Ivana. *Kriminologie*. 5., aktualizované vydání. Praha. Wolters Kluwer, 2019. s. 393-404. ISBN 978-80-7598-554-5.

[25] Kaspersky: *What is Pharming and how to protect yourself* [online]. [cit. 2022-07-22]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/pharming

[26] GŘIVNA, Tomáš, SCHEINOST, Miroslav a ZOUBKOVÁ, Ivana. *Kriminologie*. 5., aktualizované vydání. Praha. Wolters Kluwer, 2019. s. 393. ISBN 978-80-7598-554-5.

uživatel dostane na stránku odkud se okamžitě začne stahovat malware do počítače, nebo se dostane na stránku tvářící se jako legitimní stránka banky, ale po zadání přihlašovacích údajů se tyto údaje uloží do vzdálené útočníkovi databáze, a pro zmírnění podezření je uživatel následně přesměrován na opravdovou stránku své banky.

Toto jsou příklady dvou nejčastějších použití pharmingu, tedy jednak jako způsob, jak dostat výše zmíněný malware do počítače, nebo jako forma krádeže za použití lživých nebo zavádějících informací. [27]

3.1.1.3. Prolamovač hesel

Jedná se o poměrně jednoduchý typ kyberútoku, jehož úspěšnost záleží na kvalitě uživatelských hesel, neboť se jedná o software sloužící jako generátor znaků, který zkouší generovat hesla do doby, než narazí na to správné. Tedy jednoduchá krátká hesla mají větší šanci být prolomena než hesla složitějšího rázu obsahující různě velká písmena, čísla a speciální znaky. [28]

3.1.2. Virus (Malware)

Virus je typ počítačového programu, který se po spuštění začne sám replikovat. Toho dosáhne pomocí napadnutí jiného programu a vložení vlastního kódu. Jelikož tento proces probíhá bez svolení a často ani vědomosti uživatele, virus je označen jako druh škodlivého softwaru (malware).

Konečný účel počítačového viru ale může být různý. Od méně škodlivých virů, které pouze zpomalují počítač prováděním úloh na pozadí, a kterých si uživatel nemusí nikdy všimnout, přes viry určené ke krádeži financí nebo osobních údajů uživatele, až po viry určené k sabotáži systému, smazání dat anebo poškození celého počítače.

---

[27] Kaspersky: *What is Pharming and how to protect yourself* [online]. [cit. 2022-01-19]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/pharming

[28] GŘIVNA, Tomáš, SCHEINOST, Miroslav a ZOUBKOVÁ, Ivana. *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. s. 394. ISBN 978-80-7598-554-5.

Přestože se pojmem „počítačový virus“ často nesprávně označuje téměř jakýkoliv škodlivý software, počítačové viry nejsou v dnešní době tak prevalentní jako jiné druhy malwaru.

3.1.2.1. *Trojský kůň*

Trojský kůň je druh škodlivého softwaru (malware), kterého základem je oklamání uživatele o jeho opravdovém účelu. Toho dosáhne obvykle tím, že se prezentuje jako jiný program nebo soubor. Konkrétní příklad funkce může být stažitelný dokument v e-mailu tvářící se jako běžný formulář, nebo také podvodná reklama na sociálních sítích nebo jinde.

Trojský kůň jako takový nebezpečný není, používá se pouze jako prostředek k přenesení škodlivého kódu do počítače. Nejběžnějším „nákladem“ (payload) trojského koně v dnešní době je tzv. *backdoor* (zadní vstup). Laicky řečeno, je to způsob pro hackera, jak si pomocí trojského koně „otevřít vstup do počítače zevnitř“. Znamená to tedy, že po stažení trojského koně získá hacker přístup do cílového počítače, ve kterém pak může provádět celou řadu činností, podobně jako je popsáno víše v popisu počítačového viru.

Na rozdíl od viru ale trojský kůň pro svou činnost nenapadá jiné programy ani se nereplikuje (i když teoreticky hacker s pomocí trojského koně může po získání přístupu napadený počítač zavirovat).[29]

3.1.2.2. Rootkit

Rootkit je soubor softwaru používaný pro získání přístupu k jinak nepřístupným datům nebo částem počítače. „Root“ (angl. „kořen“) je označení privilegovaného účtu v Linuxových systémech, a rootkit je tedy využíván k překonávání podobných omezení, pokud uživatel (nebo, častěji, hacker) nemá relevantní přístup. Přestože se takovýto software dá použít i k nevinným účelům, například v PC servisu apod., většinou rootkit využívají právě hackeři, ať už k získání přístupu k citlivým datům, nebo získání plných administrátorských práv, a tudíž úplné kontroly nad počítačem.

---

[29] KOLOUCH, Jan a VOLEVECKÝ, Petr. *Trestněprávní ochrana před kybernetickou kriminalitou.* Praha: Policejní akademie České republiky v Praze. 2013. s. 41-44. ISBN 978-80-7251-402-1.

Ať už se do počítače dostane jakkoliv, velký problém s rootkitem, který se úspěšně spustil na napadeném počítači, je ten, že jelikož si zajistil administrátorská práva, může jednoduše ovládat a upravit nastavení jakéhokoliv antivirového softwaru, který by ho jinak mohl detekovat a smazat. Proto pokud si ho uživatel nebo antivirus nevšimne dostatečně brzo, tak většinou je následně velmi těžké počítač vyčistit a znovu zprovoznit.

Zajímavou vlastností rootkitu je to, že je to opravdu pouze nástroj na překonání určité překážky. Pokud by tedy uživatel napadeného počítače nebo technik v servisu byl dostatečně schopný, mohl by použít svůj vlastní rootkit k znovunabytí administrátorských práv, a následnému odstranění dotyčného cizího rootkitu, kterým byl počítač napaden.

Jelikož je rootkit tedy pouze nástroj, dá se kromě výše zmíněných nezákonných účelů použít i k běžným, v zásadě legálním činnostem, kupříkladu ve firemní síti ho může administrátor nainstalovat jako způsob monitorování zaměstnanců. Dalším příkladem by mohlo být domácí použití rootkitu ve formě programu pro překonání ochrany autorských práv, například CD emulátory jako PowerISO, nebo známější Daemon Tools. Není to sice zcela legální, ale pořád to z uživatele nedělá hackera.

Co už z člověka dělá hackera je moderní použití rootkitu, ne jako konečného programu, ale pouze jako prostředku pro zamaskování jiného druhu malwaru při proniknutí do cílového počítače, podobně jako trojský kůň. Kde trojský kůň používá oklamání uživatele o svém záměru, rootkit dokáže svému „nákladu“ (payloadu) zajistit potřebná práva a zároveň ho zakrýt před okem antiviru. [30] [31]

---

[30] KAPOOR, Aditya a SALLAM, Ahmed. Rootkits Part 1 of 3: *The Growing Threat*. [online]. [cit. 2022-01-22]. Dostupné z: http://download.nai.com/Products/mcafee-avert/whitepapers/akapoor_rootkits1.pdf

[31] KAPOOR, Aditya a SALLAM, Ahmed. Rootkits Part 2 of 3: *A Technical Primer*. [online]. [cit. 2022-01-22]. Dostupné z: https://www.01net.it/wp-content/uploads/sites/14/2014/10/McAfee_rootkit_windows.pdf

3.1.2.3. Spyware

Pod pojmem spyware se označuje jakýkoliv software, kterého účelem je získávání informací o uživatelově aktivitě, ať už na internetu a v prohlížeči, nebo na jeho počítači jako takovém. Spyware v dnešní době nemusí být vždy nelegální, protože většina moderních internetových korporací využívá legální verze spywaru, hlavně za účelem cílené reklamy a získávání informací o návštěvnosti svých stránek. Mezi tyto firmy zařazujeme přednostně Google a Facebook, a společně s nimi většina sociálních sítí. Informace o těchto formách spywaru se většinou nachází v dokumentu o souhlasu používání služeb, té, které stránky, nebo ve formě vyskakujícího okna „souhlasím s cookies“, apod.

Přestože jsou tyto formy spywaru legální, uživatelé si často ani neuvědomují, jaké informace jsou sbírány, jak je jejich aktivita monitorována, nebo jak je s jejich informacemi nakládáno. Jelikož ale všichni uživatelé musejí souhlasit s podmínkami použití služeb u většiny stránek, je velice obtížné vytvořit na takovémto základě jakýkoliv soudní případ. I přesto se v dnešní době tato problematika soudně řeší, příkladem nedávný proces s ředitelem Facebooku Markem Zuckerbergem ohledně zpronevěry informací uživatelů Facebooku firmě Cambridge Analytica. [32]

Závažnější formou spywaru je pak tzv. *keylogger,* což je software, který zachycuje a nahrává stisky kláves na klávesnici. Přestože takovýto software není nelegální, a dá se použít i jako forma monitorování zaměstnanců ve firmě, ve většině případů se používá jako způsob k odcizení hesel, kódů, a dalších přihlašovacích údajů a podobných citlivých informací podobně jako prolamovače hesel.

Do počítače se může dostat jako jakýkoliv jiný malware, například jedním ze způsobů popsaných výše. Antivirové programy mají většinou s keyloggery a spywarem obecně problém, protože většina z nich není v zásadě nelegální, a

[32] Spyware Workshop: *Monitoring Software On Your Personal Computer: Spyware, Adware, and Other Software: Report of the Federal Trade Commission Staff*“. [online]. [cit. 2022-07-25]. Dostupné z: https://www.ftc.gov/reports/spyware-workshop-monitoring-software-your-personal-computer-spyware-adware-other-software

uživatel si je mohl nainstalovat sám. Na odstranění spywaru se proto používají specializovanější programy s kolektivním názvem *anti-spyware*. [33]

3.1.2.4. Ransomware

Jakýkoliv software, který se používá k vydírání uživatele, se označuje pojmem „ransomware“, od anglického slova *ransom* – výkupné. Ve své podstatě malware, u ransomware nejde o to, jak se dostane do počítače nebo jak přesně funguje, ale spíše co je jeho účel – tedy odepření přístupu uživatele od určitých dat nebo od celého počítače, a požadování určité finanční částky za jeho navrácení.

Přístup může být odepřen buďto prostým zaheslováním, nebo v závažnějších případech zašifrováním, s různou komplexností použitého šifrování. Často se hacker snaží přelstít uživatele tím, že svůj ransomware vydává za něco oficiálního (například policii), a snaží se uživatele dostatečně vyděsit na to, aby zaplatil požadovanou částku (malware určený k zastrašování uživatelů se nazývá také scareware). Po převedení peněz, obvykle nějakým anonymním způsobem, je v hackerově nejlepším zájmu navrátit přístup uživateli; pokud by to neudělal, a podobným způsobem okradl více lidí, postupně by ho lidé mohli přestali brát vážně a přestali by mu posílat peníze. [34]

3.1.2.5. Červ

Z anglického *worm*, tento škodlivý program se, podobně jako virus, sám replikuje, ale, na rozdíl od viru, na to nepotřebuje napadnout jiný program nebo kamkoliv vkládat svůj kód. Nejvýznamnější vlastností počítačového červa je ale způsob jeho šíření. Jakmile se červ octne na cílovém počítači (ať už se tam dostal pomocí trojského koně nebo jiným způsobem), začne prohledávat síť, ve které je infikovaný počítač zapojený, a hledat další počítače, na které by se mohl

---

[33] GREBENNIKOV, Nikolay. *„Keyloggers: How they work and how to detect them (Part 1)“.* [online]. [cit. 2022-01-22]. Dostupné z: https://securelist.com/keyloggers-how-they-work-and-how-to-detect-them-part-1/36138/

[34] KOLOUCH, Jan a VOLEVECKÝ, Petr. *Trestněprávní ochrana před kybernetickou kriminalitou.* Praha: Policejní akademie České republiky v Praze, 2013. s. 40-41. ISBN 978-80-7251-402-1.

zkopírovat. Pokud je další počítač nalezen a červ zkopírován, proces začíná znovu a takto jsou exponenciálním způsobem postupně nakaženy všechny počítače v síti.

Jak bylo zmíněno na začátku, červ na rozdíl od viru nijak nepoškozuje systémy, ve kterých se nachází a kterými prochází. Červi kromě svého sebe šířícího poslání s sebou většinou žádný další škodlivý kód nenesou, a dalo by se říct, že na velmi malých sítích jsou takřka neškodné. Jejich konečný účel ale spočívá v tom, že svojí činností zpomalují síť, ve které se nachází, což, v případě větších sítí, může mít za následek její přetížení a výpadek, což se také nazývá **DDoS**. [35] [36]

3.1.3. Omezování dostupnosti služeb

3.1.3.1. *DoS a DDoS útoky*

DoS (Denial of service) a DDoS (Distributed denial of service) nemají za cíl dostat se k nějakým informacím či překonat bezpečností prvky naopak se snaží o omezení přístupu na server. Útoky jsou používány k odepírání konkrétních služeb na internetu tím, že server provozující danou službu zahltí v krátkém časovém úseku nezpracovatelným množstvím požadavků a tím docílí dočasné odepření jeho služeb.

Nejčastěji se k tomuto útoku využívá sítě počítačů známé jako Botnet. Do sítě Botnet je síť zařízení připojených k internetu, jako jsou počítače, chytré telefony nebo jiných zařízení schopných internetového připojení jejichž zabezpečení bylo prolomeno například pomocí backdoor payloadu, který na zařízení dostal zmiňovaný trojský kůň a jejichž kontrolu má v rukou útočník nebo třetí strana kterou útočník může využít. Každé kompromitované zařízení, se stává "botem" v této síti a je nyní možné přes tento botnet posílat požadavky ve větším množství a mnohem intenzivněji.

---

[35] Kaspersky: *What is a Computer Virus or a Computer Worm?* [online]. [cit. 2022-02-04]. Dostupné z: https://www.kaspersky.co.uk/resource-center/threats/viruses-worms

[36] KREMLING, Janine a PARKER, Amanda M. S. Cyberspace, cybersecurity, and cybercrime. London;Washington DC;New Delhi;Los Angeles;Singapore;Melbourne;: SAGE, 2018. s. 50-51. ISBN 9781506347257;1506347258;

Jedny z nejznámějších botnet sítí jsou LOIC (Low Orbit Ion Cannon) a HOIC (High Orbit Ion Cannon). Tyto botnety jsou legálním prostředkem k testování odolnosti proti DoS a DDos útokům. [37]

3.2. Útoky spočívající v šíření škodlivého obsahu

3.2.1. Šíření dětské pornografie, Sexting,

Dětská pornografie je nyní kvůli internetu poměrně závažným problémem právě kvůli její snadné distribuci a poměrně snadná dostupnosti nejen na Darkwebu.

„Úmluva o kybernetické kriminalitě zahrnuje pod škodlivý obsah na internetu problematiku dětské pornografie, tj. takové, která zobrazuje nebo jinak využívá dítě nebo osobu, jež se jeví dítětem. Trestním zákonem je postihováno jakékoliv nakládání s dětskou pornografií od získávání přístupu k ní po výrobu a distribuci.“

K problémům s dětskou pornografií neodmyslitelně patří i takzvaný sexting kdy dochází k dětské prostituci často za úplatu, výměnou za jiné fotografie, zmanipulováním nezletilé oběti či pod pohrůžkou násilí. Focení intimních partií nahrávaní videí atd., to vše je sexting a jakékoliv šíření nebo úmyslné obstarávaní si takovýchto medií je trestným činem. Není nezvyklé, že se takovýto sexting často změní na kybergrooming. [38]

3.2.2. Kybergrooming

Podstatou kybergroomingu je psychická manipulace dětí dospělými za použití prostředků informačních technologií s cílem získání důvěry domluvy osobní schůzky, na které se pachatel zpravidla pokusí oběť znásilnit či jinak sexuálně zneužít. S tímto útokem se nejčastěji setkáváme na internetových seznamkách, sociálních sítích nebo jen v rámci chatovacích programů[39]

---

[37] KOLOUCH, Jan a VOLEVECKÝ, Petr. *Trestněprávní ochrana před kybernetickou kriminalitou.* Praha: Policejní akademie České republiky v Praze. 2013. s. 47-49. ISBN 978-80-7251-402-1.

[38] GŘIVNA, Tomáš, SCHEINOST, Miroslav a ZOUBKOVÁ, Ivana. *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. s. 397. ISBN 978-80-7598-554-5.

[39] Internetem bezpečně: *Kybergrooming* [online]. [cit. 2022-08-06]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybergrooming/

3.2.3. Kyberstalking

Stejně jako stalking tradiční se jedná o nebezpečné pronásledování oběti pachatelem, avšak za v tomto případě je to za použití prostředků informačních technologií. Jedná se o dlouhodobé, opakované a stupňované kontaktování – pronásledování své oběti, ve které chce úmyslně vyvolat pocit strachu o své soukromí, zdraví nebo život. Pachatel k dosažení svého cíle například opakovaně zasílá oběti SMS zprávy, oběti volá nebo ji jen prozvání, často komentuje příspěvky oběti na sociálních sítích, anebo se uchyluje ke krádeži identity oběti a vystupuje pak jejím jménem.[40]

3.2.4. Extremismus

V rámci dodatku č. 189 k Úmluvě o kybernetické kriminalitě byli přidány také postihy za počítačové šíření rasové a xenofobní nenávisti, rasově a xenofobně motivované urážky a výhružky, popírání nebo hrubé zlehčování, schvalování nebo ospravedlňování genocidy či zločinů proti lidskosti.[41]

Takovéto formy extremismu nejsou na internetu nijak vzácné vzhledem k množství sociálních sítí, které jsou nyní dostupné je poměrně snadné založit skupinu podobně smýšlejících a navzájem se podporujících lidí.

Mezi takovéto skupiny patří popírači holocaustu, veřejní příznivci totalitních režimů porušující lidská práva ať už režimů z minulosti nebo režimů novodobých. Rasově a xenofobně motivované skupiny jako jsou skinheads nebo neonacistické skupiny.

Veřejní zastánci násilí na rasových menšinách. Konkrétním příkladem je B. Čermák, který byl odsouzen za online schvalování rasové motivovaného útoku na mešity ve městě Christchurch na Novém Zélandu. Na internetové diskusi komentoval tuto událost slovy „Jak jim chutná jejich medicína. Dobrá práce???!“.

---

[40] Internetem bezpečně: *Kyberstalking* [online]. [cit. 2022-08-06]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kyberstalking/

[41] Kapitola II., články 3,4,5,6, Dodatkového protokol k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů.

Podle soudce jasně šlo o pochvalu spíše než o kritiku a B. Čermák byl odsouzen bezpodmínečně na šest let vězení.[42]

3.2.5. Kyberterorismus

I přesto, že se Úmluva o kybernetické kriminalitě tohoto tématu nedotýká této skupiny útoků a trestných činů lze také zařadit kyberterorismus.

Abychom se mohli bavit o kyberterorismu musíme nejdříve definovat co je terorismus jako takový - *„**Terorismus** je plánované, promyšlené a politicky motivované násilí, zaměřené proti nezúčastněným osobám, sloužící k dosažení vytčených cílů.“*[43]

„Kyberterorismus – je *konvergencí terorismu a kyberprostoru, obecně chápaný jako nezákonný útok nebo nebezpečí útoku proti počítačům, počítačovým sítím a informacím v nich skladovaným v případě, že útok je veden s cílem zastrašit nebo donutit vládu, nebo obyvatele k podporování sociálních nebo politických cílů.“*[44]

Hlavním rozdílem mezi kyberterorismem a terorismem je, že kyberterorismus používá informační technologie jako hlavní, při čistě digitálních operacích jediný, prostředek pro dosažení svých cílů.

Mezi cíle můžeme řadit – snahu o přístup k utajovaným datům k zneužití čí zničení, pomocí DDoS útoků napadat kritickou infrastrukturu jako ropovody, elektrárny, průmysl, ale také útoky na banky a jiné finanční instituce ať už k získání finančních prostředků nebo ve snaze o kolaps ekonomického systému.

Teroristické organizace využívají kyberprostor také k šifrované komunikaci mezi sebou, k šíření své propagandy, hledání nových členů či sympatizantů.[45]

---

[42] Novinky.cz: *Tvrdý trest za schvalování terorismu na internetu. Muž dostal šest let vězení* [online]. [cit. 2021-03-16, v čase 15:07]. Dostupné z: https://www.novinky.cz/krimi/clanek/tvrdy-trest-za-schvalovani-terorismu-na-internetu-muz-dostal-sest-let-vezeni-40354135

[43] Ministerstvo vnitra České republiky MV ČR: Definice pojmu terorismus [online]. [cit. 2022-01-16]. Dostupné z: https://www.mvcr.cz/clanek/definice-pojmu-terorismus.aspx.

[44] DENNING, Dorothy E. Definice pojmu kyberterorismus [online]. [cit. 2021-01-16]. Dostupné z: https://fas.org/irp/congress/2000_hr/00-05-23denning.htm

[45] KOLOUCH, Jan a VOLEVECKÝ, Petr. *Trestněprávní ochrana před kybernetickou kriminalitou.* Praha: Policejní akademie České republiky v Praze, 2013. s. 55-57. ISBN 978-80-7251-402-1.

3.2.6. Fake news a hoax, škodlivé návody, spam,

3.2.6.1. Fake news a hoax

V posledních pár letech se také setkáváme s fenoménem šíření fake news. „Fake news lze definovat jako zprávy obsahující nepravdivé nepřesné nebo manipulativní informace s cílem poškodit konkrétní osobu organizaci nebo stát.“[46] Obzvláště během pandemické situace ohledně COVID-19, vznikaly zprávy, které měli obyvatelé odradit od očkování, zprávy zpochybňující existenci viru Covid-19 anebo třeba zprávy tvrdící, že vakcína obsahuje mikročip pro připojení lidí do 5G sítě. Fake news je i pouhé pro zábavu učiněné oznámení záchranným nebo bezpečnostním sborům, které zapříčiní jejich bezdůvodný výjezd.

Šíření fake news (poplašné zprávy) je trestné dle §357 odst. 1 a 2, Trestního zákoníku ve znění: „(1) *Kdo úmyslně způsobí nebezpečí vážného znepokojení alespoň části obyvatelstva nějakého místa tím, že rozšiřuje poplašnou zprávu, která je nepravdivá, bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti. (2) Kdo zprávu uvedenou v odstavci 1 nebo jinou nepravdivou zprávu, která je způsobilá vyvolat opatření vedoucí k nebezpečí vážného znepokojení alespoň části obyvatelstva nějakého místa anebo bezdůvodnou záchrannou práci integrovaného záchranného systému sdělí soudu, orgánu Policie České republiky, orgánu státní správy, územní samosprávy, nebo jinému orgánu veřejné moci, právnické osobě, fyzické osobě, která je podnikatelem, anebo hromadnému informačnímu prostředku, bude potrestán odnětím svobody na šest měsíců až tři léta nebo zákazem činnosti.“* [47]

3.2.6.2. Škodlivé návody

Jako škodlivý návod můžeme chápat, jakékoliv návody popisující, jak spáchat konkrétní trestný čin nebo třeba návody, jak utajovat trestnou činnost. Návody sloužící k výrobě zbraní, drog, výbušnin a jiných předmětů nelegální

[46] GŘIVNA, Tomáš, SCHEINOST, Miroslav a ZOUBKOVÁ, Ivana. Kriminologie. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. s. 399. ISBN 978-80-7598-554-5.
[47] *Trestní zákoník* [online]. [cit. 2022-02-08]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

povahy. Někdy se lze setkat i s návody, kde autor záměrně uvádí špatné postupy, aby osoba postupující podle nich přišla k nějaké újmě.[48]

3.2.6.3. Spam

Spam je kybernetickým útokem, který sám o sobě nutně nepředstavuje velkou hrozbu, pokud mu člověk nevěnuje přílišnou pozornost. Spam bývá povětšinou hromadná nevyžádaná zpráva, reklamního charakteru, která je nejčastěji šířena v rámci elektronické komunikace převážně emaily a SMS. Avšak v některých případech se může jednat o nevyžádanou zprávu která může být doprovázena nějakým virem, který se po otevření zprávy nebo kliknutím na odkaz ve zprávě může stáhnout do počítačového systému.[49]

3.3. Útoky spočívající v porušování práv duševního vlastnictví

Internet umožňuje sdílet nejrůznější věci téměř okamžitě, v posledních letech vzniklo hned několik internetových platforem pro sdílení komerčních autorských děl. Avšak toto pozitivum globálnosti a dostupnosti internetových služeb, také usnadňuje skoro až vybízí, k nelegální elektronické krádeži a poté distribuci autorsky chráněných materiálů. Primárně je distribuce prováděna na veřejných úložištích kde pachatel nahraje ukradený materiál a ostatní uživatelé poté mohou získat jeho stažením do počítače. [50]

Jedním z dalších způsobů, jak se uživatel dostane k takovému obsahu je takzvaný torrenting. Torrenting funguje na principu peer-to-peer kdy si uživatel stáhne soubor typu .torrent, který má v sobě uložena metadata a sledovače umožňující přístup na konkrétní místo v kyberprostoru kde se soubor nachází a z toho jej stáhnout bez potřeby se připojení ke konkrétnímu centralizovanému uložišti. [51]

---

[48] GŘIVNA, Tomáš, SCHEINOST, Miroslav a ZOUBKOVÁ, Ivana. *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. s. 399. ISBN 978-80-7598-554-5

[49] KOLOUCH, Jan a VOLEVECKÝ, Petr. *Trestněprávní ochrana před kybernetickou kriminalitou.* Praha: Policejní akademie České republiky v Praze, 2013. s. 33-36. ISBN 978-80-7251-402-1.

[50] GŘIVNA, Tomáš, SCHEINOST, Miroslav a ZOUBKOVÁ, Ivana. *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. s. 400. ISBN 978-80-7598-554-5

[51] Techslang: Torrenting: What is It and How does It Work? [online]. [cit. 2022-02-09]. Dostupné z: https://www.techslang.com/torrenting-what-is-it-and-how-does-it-work/

Nesmíme opomenout ani klasickou formu šíření na fyzických datových nosičích jako jsou CD/DVD nebo USB flash disky, nebo promítaní či šíření nelicencovaných nelegálně opatřených autorských děl.

Těmto pachatelům říkáme crackeři od slova cracking. Cracking spočívá v obcházení bezpečnostních prvků, které znemožňují vyrobit jakoukoliv kopii konkrétního autorského díla. Tyto prostředky se využívají k ochraně autorských práv, jak je uvedeno v *§43 odst. 1 zákona č.121/2000 Sb., autorský zákon.*

Další formou crackingu může být password cracking, která slouží ke získání přístupu do licencovaných programů a systémů. Vytvořením cracku či rozšířením nelegálně získaného generátoru klíčů (keygen) k daným autorsky chráněným dílům a tím je nelegálně zpřístupnit. Tyto cracky a keygeny jsou šířeny především na již zmíněných torrent peer-to-peer sítích.

Pachatel prolamující ochranu počítačových systémů a programů s vidinou zisku informací a neoprávněné užití těchto informací, naplňuje skutkovou podstatu trestného činu dle *§230 odst. 1 a 2 zákona č. 40/2009 Sb., Trestní zákoník konkrétně „Neoprávněný přístup k počítačovému systému a nosiči informací“*. Zpřístupněním díla chráněného autorským zákonem dochází k naplnění skutkové podstaty trestného činu *„Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi“ podle § 270 téže podle trestního zákoníku.* [52]

Motivace pachatelů těchto trestných činů *„bývá v zásadě trojího typu: zisk, ukázka vlastních schopností, posilování ideje internetu jako prostoru svobodného sdílení myšlenek všech.“* [53]

3.4. Tradiční kriminalita v kyberprostoru

3.4.1. Podvody

Internetové podvody jsou jedny z nejčastějších trestných činů v kyberprostoru, a to především v oblasti internetového obchodovaní. V rámci těchto trestných činů se využívá zejména důvěřivosti uživatelů, kteří dopředu

[52] KOLOUCH, Jan a VOLEVECKÝ, Petr. Trestněprávní ochrana před kybernetickou kriminalitou. Praha: Policejní akademie České republiky v Praze, 2013. s. 52. ISBN 978-80-7251-402-1.
[53] GŘIVNA, Tomáš, SCHEINOST, Miroslav a ZOUBKOVÁ, Ivana. *Kriminologie*. 5., aktualizované vydání. Praha. Wolters Kluwer, 2019. s. 400. ISBN 978-80-7598-554-5.

zaplatí za zboží, které pachatel nabízí ať už na bazarech nebo na podvržených e-shopech. Pachatel láká uživatele hlavně na překvapivě výhodné zboží, které však vůbec nemusí dorazit, je jiné, než za které uživatel zaplatil nebo je velice nekvalitní. [54]

3.4.2. Carding, card skimming

3.4.2.1. Carding

Carding je velice běžným zneužitím platební karty, jedná se o placení online transakcí, kdy není zapotřebí mít platební kartu fyzicky k tomu, aby mohla platba proběhnout. Stačí tedy znát číslo karty, expirace, a CVV kód na zadní straně kreditní karty, který primárně slouží proti takovémuto zneužití. S těmito informacemi pak pachatel může do určitého limitu nastaveného uživatelem nakupovat na internetu. Velice často se s kradenými PayPal účty, kreditkami nebo jejich údaji setkáváme na černých trzích skrývajících se na dark webu.

3.4.2.2. Card skimming

Card skimming už je poněkud sofistikovanější proces krádeže platební karty. Spočívá v krádeži dat uložených na platebním prostředku, ať už jde o kreditní, debetní nebo jinou kartu. S těmito daty je poté pachatel schopen vytvořit padělanou kreditní kartu na, kterou nahraje ukradená data což umožní s padělanou kartu používat stejně jako kartu pravou, avšak peníze se odečítají z účtu oběti. [55]

3.4.2. Ostatní trestná činnost

3.4.2.1. *Krádež identity*

Za zmínku stojí například krádež identity, která je v porovnání se světem reálným poněkud snazší v kyberprostoru, vzhledem k době, kdy téměř každý po sobě zanechává na internetu digitální stopy v podobě osobních údajů např. vlastního jména a velice často i fotografie na sociální síti. Jen tyto dvě věci stačí

---

[54] GŘIVNA, Tomáš, SCHEINOST, Miroslav a ZOUBKOVÁ, Ivana. *Kriminologie*. 5., aktualizované vydání. Praha. Wolters Kluwer, 2019. s. 401. ISBN 978-80-7598-554-5.

[55] KOLOUCH, Jan a VOLEVECKÝ, Petr. Trestněprávní ochrana před kybernetickou kriminalitou. Praha: Policejní akademie České republiky v Praze, 2013. s. 57-64. ISBN 978-80-7251-402-1.

k tomu, aby se pachatel mohl velice snadno vydávat za někoho kým ve skutečnosti není.[56]

3.4.2.1. *Legalizace výnosů z trestné činnosti*

Tato činnost je převážně známa jako praní špinavých peněz (money laundering) „…*proces, během kterého je zamlžen nebo zastřen jejich původ tak, aby se zdálo, že jde o peníze získané legální cestou…*“[57]

Vzhledem k rapidním nárůstu počtu kryptoměn v posledních letech je velice populární prát špinavé peníze za pomoci těchto kryptoměn jako je například bitcoin. Kryptoměny zlehčují zakrývání opravdového zdroje příjmu z trestné činnosti, neboť nabízejí anonymitu, velice snadné užití a je díky nim možné obcházet státní ale i mezinárodní regulace a předpisy. Tento fakt zapříčinil nebývalou popularitu u pachatelů kybernetické trestné činnosti a jsou nyní často vyžadovány u kyberútoků jako je například ransomware nebo při obchodu s nelegálním zbožím na virtuálních černých trzích. [58]

Zajímavostí je, že se k praní špinavých peněz využívají i online videohry jako je například World of Warcraft kde dochází ke směně reálných peněz za herní měnu. A to tak, že pachatel si od jiného hráče koupí herní měnu za reálné peníze a takto získanou herní měnu pak prodá dalšímu jinému hráči opět za reálné peníze. Nutno však podotknou, že ve většině videoher je jakákoliv prodej služeb předmětů nebo herní měny postihnutelný na základě Licenční smlouvy s koncovým uživatelem. I když konkrétně ve hře World of Warcraft lze koupit herní měnu i za reálné peníze skrze token, který sami vývojáři do hry přidali. Jakýkoliv následný prodej herní měny je však je penalizovatelný.[59]

---

[56] GŘIVNA, Tomáš, SCHEINOST Miroslav a ZOUBKOVÁ Ivana. *Kriminologie*. 5., aktualizované vydání. Praha. Wolters Kluwer, 2019. s. 402. ISBN 978-80-7598-554-5.

[57]Finanční vzdělávání: *Praní špinavých peněz*. [online]. [cit. 2022-08-15]. Dostupné z: https://www.financnivzdelavani.cz/svet-financi/bankovnictvi/prani-spinavych-penez

[58] MARKS, Jonathan T. „Cryptocurrency and money laundering: why understanding fraud is critical“ [online]. [cit. 2021-11-15]. Dostupné z: https://www.bakertilly.com/insights/cryptocurrency-and-money-laundering

[59] IRWIN, Angela a SLAY, Jill. 2012. Detecting Money Laundering and Terrorism Financing Activity in Second Life and World of Warcraft. International Cyber Resilience conference.

3.4.3. Černý trh

Další trestnou činností v kyberprostoru je provozování virtuálních černých trhů zvané jako „Darknet markets“, které jsou schovávané na darkwebu a slouží primárně k nákupu a prodeji nepovoleného zboží. Hlavně je řeč o drogách, již zmíněných kreditních kartách, padělaných dokumentech a penězích, zbraních a různých běžně nedostupných farmaceutikách.

Avšak na darkwebu lze koupit i více než jen nelegální zboží, na darkwebu probíhá obchod s lidmi, hlavně se ženami, které se prodávají jako otrokyně primárně k sexuálním účelům ale i dětmi, které se též, ač k velkému znepokojení, prodávají jako sexuální otroci.

Dále se dají nakoupit i různé služby od najmutím hackerů, přes ublížení na zdraví specifické osobě, po vraždu.

4. Prevence kyberkriminality

Ochrana před kybernetickou kriminalitou je v první řadě založena na efektivní prevenci jakéhokoliv bezpečnostního incidentu prostřednictvím, různé osvětové činnosti pro veřejnost, školení zaměstnanců, fyzickou ochranou, softwarovou nebo hardwarovou ochranou či užitím etických hackerů.

4.1. Software ochrana

4.1.1. Firewall, antivirové programy,

4.1.1.1. Firewall

Firewall je bezpečností zařízení, které může mít jak softwarovou, tak hardwarovou podobu a pomáhá chránit uživatelskou síť před neoprávněným připojením k počítači, či pokusům malware útoků na počítač. Toho dosáhne tak, že kontroluje a filtruje provoz na síti, tedy jednak blokuje příchozí nevyžádanou a potencionálně škodlivou síťovou komunikaci, ale dokáže také zastavit odchozí pokusy o odchozí komunikaci, což je převážně případ softwarových firewall. Dnes již každý běžný operační systém obsahuje předinstalovaný ochranný prvek firewall. Softwarovým firewallem se rozumí program nainstalovaný v počítači,

hardwarový firewall je například router, ale dá se také pořídit jako samostatná jednotka. [60]

4.1.1.2. *Antivirus*

Antivirus je program, který na rozdíl od firewall nutně nemusí filtrovat příchozí požadavky, nýbrž skenuje obsah, který se již nachází na počítači v zájmu nalezení potencionálně nebezpečných souborů. Nalezené soubory pak uzavře do tzv. karantény a vyčká na uživatelovo rozhodnutí co se souborem udělat, popřípadě jej rovnou smaže.[61] Mnoho antivirových programů je součástí větších balíčků softwaru, které mohou kromě antivirového programu obsahovat také například antispam v emailové schránce, zabezpečení internetového prohlížeče a domácí sítě, nebo správce hesel.

4.1.2. Zálohování

Zálohování funguje na principu vytváření kopií dat, aby v případě jejich nedostupnosti, odcizení nebo ztráty byly stále k dispozici. Klíčové pro zálohy je pravidelnost jejich vytváření a samozřejmě jejich zabezpečení. Vzhledem k množství dat, ukládaných na běžně používaných zařízeních jako jsou telefony notebooky a počítače, by měl uživatel tyto data zálohovat, pravidelně na místo jiné než úložiště těchto zařízení, ať už se jedná o fotografie, lékařské nebo finanční dokumenty nebo jiné osobní údaje. Ideálním fyzickým zařízením, kam data uložit je například flashdisk, CD/DVD, externí harddisky či jen prosté papírové kopie. Pokud uživateli nevyhovuje fyzická záloha existují i online zálohovací služby, které za úplatu data zálohují a šifrují na svých serverech.[62]

4.1.3. Uzamčení přístupu

Toto zahrnuje klasické použití hesla nebo PIN kódu k odemčení přístupu k zařízení, účtu, nebo datům. Přestože se na první pohled můžou zdát banální, hesla a kódy jsou nejčastěji využívanou formou ochrany před nepovoleným

---

[60] JOHANSEN, Alison Grace. „What is a firewall? Firewalls explained and why you need one.“ [online]. [cit. 2021-06-17]. Dostupné z: https://us.norton.com/internetsecurity-emerging-threats-what-is-firewall.html

[61] JOHANSEN, Alison Grace. „What is antivirus software? Antivirus definition.“ [online]. [cit. 2019-02-22]. Dostupné z: https://us.norton.com/internetsecurity-emerging-threats-what-is-firewall.html

[62] National cybersecurity alliance: „Back it up“ [online]. Dostupné z: https://staysafeonline.org/stay-safe-online/online-safety-basics/back-it-up/

přístupem, ať už k zařízení jako takovému (PC, laptop, mobilní telefon), nebo na digitální úrovni, jako přístup k datům nebo uživatelským účtům.

Kromě hesla nebo kódu se v dnešní době využívá také biometrika, což zahrnuje snímání otisku prstu, snímání obličeje, nebo také hlasu.

4.1.4. Šifrování dat

„Šifrování je základním stavebním prvkem zabezpečení dat. Je to nejjednodušší a nejdůležitější způsob, jak zajistit, aby informace z počítačového systému nemohl odcizit a přečíst někdo, kdo je chce použít ke škodlivým účelům.“[63]

Šifrování v oblasti kybernetické bezpečnosti spočívá v převodu standartně čitelných dat do dat zašifrovaných. Zašifrovaná data pak může uživatel přečíst nebo zpracovávat až po jejich dešifrování. K dešifrování dat je zapotřebí kryptografického klíče, který je uložen na serveru kde se zašifrovaná data posílají, a tudíž umožňuje uživatelům v rámci sítě dešifrovat příchozí data.

Standardně je používá buď symetrické šifrování kde klíč k zašifrování je stejný jako k dešifrování, anebo asymetrické šifrování, u kterého jsou zapotřebí dva různé klíče, jeden k šifrování a druhý k dešifrování.

4.1.5. User management

User managment je nedílnou součástí každé zabezpečené soukromé sítě. Jde o řízení přístupu a oprávnění uživatelů ke konkrétním datům uložených v rámci sítě. Na základě těchto oprávnění systém poté povoluje nebo naopak zakazuje přístup k aplikacím, databázím či jiným datům.

Ve větších, zejména nedomácích, sítích se také často využívá takzvaný radič domény (domain controller, DC). Radič domény je server, která má na starosti vyřizování bezpečnostních požadavků v síti, zpravidla tedy požadavků jiných počítačů na přístup k doménovým prostředkům. Kromě toho má doménový

---

[63] Kaspersky: *What is data encryption?* [online]. [cit. 2022-07-22]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/encryption

řadič na starosti nastavení přístupů uživatelských účtů a obecnou bezpečnostní politiku sítě jako takové. [64]

Příkladem; v případě, že si uživatel v síťové doméně zažádá o přístup k nějakým prostředkům, doménový řadič nejprve zkontroluje, zda k tomuto obsahu dotyčný uživatel vůbec má přístup, a poté ho buďto autentizuje, tedy mu poskytne přístup, nebo nikoliv, podle bezpečnostní politiky nastavené správcem sítě.

Nejčastěji využívaným typem řadiče domény je Active Directory, vyvinutý společností Microsoft pro operační systémy Windows. [65]

4.1.6. Monitoring/logování

Monitoring spočívá v neustálém monitorování systému, uživatelů a jejich aktivit, primárně za účelem prevence bezpečnostních incidentů. Monitorovaná aktivita je evidována ve formě logu k případné analýze bezpečnostního incidentu nebo jako důkazní materiál.

Monitoring a logování většinou nejsou součástí běžného zabezpečení domácí sítě, nýbrž jsou hojně využívané ve firmách a společnostech, obzvláště v těch, které musí provozovat svoje služby neustále, tzv. „provoz 24/7“. Dobrým příkladem firmy s takovýmto provozem jsou banky. V dnešních moderních bankách, které mají velkou většinu svého fungování zdigitalizovanou, je monitoring a logování velice důležité.

Mnoho těchto digitálních bankovních procesů se nezastaví ani v noci, například automatická denní uzávěrka a procesy s ní spojené, proto mají banky většinou vyhrazené IT zaměstnance, kteří jsou „na příjmu“ i přes noc, a mohou tedy okamžitě zasáhnout, ať už v případě nějaké chyby nebo výpadku, nebo i případného napadení. Toto je jim umožněno díky monitorovacím systémům, které např. sledují hodnoty aktivity v síti, a pokud tyto hodnoty překročí určitou úroveň

---

[65] BLANTON, Sean. „What is user management?“ [online]. [cit. 2021-10-02]. Dostupné z: https://jumpcloud.com/blog/what-is-user-management

nebo zaznamenají neobvyklou aktivitu, monitorovací program upozorní operátora, standartně pomocí SMS nebo emailu. [66]

4.2. Hardware ochrana

Hardware ochrana zahrnuje veškeré prostředky použitelné k zamezení ztráty dat a datových nosičů na fyzické úrovni.

V běžných domácích podmínkách to může znamenat fyzický zámek počítače, jako je bezpečnostní kabel, nebo také fyzický přístupový token, používaný ke generování periodicky se měnícího hesla.

Ve větších serverových místnostech a datových skladech se nicméně využívá mnohem komplexnější ochrany.

V případě výpadku elektrického proudu se používají záložní generátory elektrické energie.

Při výskytu požáru v datových centrech není možné použít klasických hasících prostředků tak, aby nedošlo k poškození hardwaru a potenciálně ke ztrátě dat. Bývá zde proto nainstalován speciální hasící systém, který k hašení plamenů využívá plynů jako dusík nebo oxid uhličitý, kterým se kompletně vyplní celá místnost, čímž se vypuklý požár uhasí. Při tomto se v prostorech nesmí nacházet žádný člověk, neboť mu hrozí těžká újma na zdraví, v krajním případě až smrt. Při detekci požáru se proto ozve výstraha, aby všichni přítomní okamžitě opustili prostory, a po určené době se objekt uzavře.

Pro zamezení poškození hardwaru statickou elektřinou mohou být podlahy pokryty uzemňovacím materiálem.

Ať už v malých serverových místnostech nebo mnohopatrových, více halových serverových polích, jelikož servery při svém fungování generují velké množství tepla, pro jejich správnou funkci je zapotřebí je ochlazovat pomocí klimatizace anebo jiných chladících systémů.

---

[66] Sentient digital, inc.: „What is cyber monitoring?“ [online]. [cit. 2021-10-05]. Dostupné z: https://sdi.ai/blog/what-is-cyber-monitoring/

Již zmíněné zálohování dat na fyzické nosiče by se také dalo nazvat hardwarovou ochranou.

4.3. Využití etických hackerů

Další z možností ochrany před kybernetickými útoky je využití etických hackerů tzv. white hats, tedy hacker, jehož motivace není škodlivá ba naopak. Tito etičtí hackeři jsou povětšinou zaměstnáni nebo najati v rámci společnosti, neboť využívají stejných postupů a prostředků jako hackeři, které ve správných rukou mohou pomoci k odhalení slabých míst či programových chyb systému.

Základní myšlenkou etického hackingu i přes to, že činnost hackera a etického hackera je velice podobné, etický hacker nevyužije nalezené bezpečností hrozby ve svůj prospěch, ale spolupracuje se společností nebo majiteli konkrétního programu, jehož bezpečnost testuje, na odstranění závad ohrožující bezpečnost dat a společnosti dříve, než dojde k jejich zneužití, a tedy i k bezpečnostnímu incidentu.

Na odhalení bezpečnostních nedostatků tedy etický hacker dostává povolení od společnosti či majitele což legalizuje jeho následnou aktivitu, a pouští se do práce. Mezi nejběžnější formy testování patří penetrační testování, jehož cílem je zjištění slabých míst potencionálně využitelných k infiltraci systému. Dále zátěžové testování, které testuje odolnost systému nejenom proti DDoS útokům, nebo obecné bezpečnostní testování. Vzhledem ke velice podobnému setu schopností, jaké mají hackeři a etičtí hackeři se tyto testy realizují pomocí simulací specifických druhů útoků. Nutné je mít aplikace zabezpečené ještě předtím, než budou přístupné potencionálním uživatelům, nicméně etický hacking nebývá jednorázovou záležitostí, nýbrž dlouhodobou spoluprací, neboť je potřeba bezpečnost testovat pravidelně u každého updatu aplikace či systému. [67]

[67] KOVALČÍK, Marek. *Etický hacking – laicky a jednoduše: Tři typy hackerů.* BDO [online]. 2020. Dostupné z: https://www.bdo.cz/cs-cz/archiv/it-security/12-2020/eticky-hacking-%E2%80%93-laicky-a-jednoduse

4.4. Osobní ochrana

Osobní ochranou rozumíme, že by měl uživatel dodržovat všeobecně známá základní pravidla při používaní internetu. Mezi taková všeobecná pravidla pro ať už jednotlivce či společnosti řadíme, dostatečně silná hesla a jiná zabezpečení profilů, dbát zvýšené opatrnosti při manipulaci s neznámými přílohami, nesdílet data svá nebo svých blízkých tam kde je k nim snadný přístup, udržovat aktualizovaný software a hardware, používání legálního softwaru atd.

Obecně lze říci, že každý uživatel by měl být při práci na počítači a internetu opatrný, nedůvěřovat všemu co vidí, pochybné weby si ověřit, nesdělovat nikomu své osobní údaje atd. V rámci zaměstnaní by navíc měl vždy dbát na bezpečností politiku společnosti či organizace a její pokyny ohledně chování na internetu.

Výše zmíněná pravidla se sice mohou zdát dospělým jasná nicméně ve větším ohrožení jsou děti. [68] Děti si zpravidla softwarovou nebo hardwarovou ochranu nezajistí a nemusí vědět, co je na internetu považováno za normální chování a co ne. Je tedy na rodičích, školách či různých organizacích předat dětem informace, jak se na internetu chovat a jaké nebezpečí na ně může v kyberprostoru čekat.

Mezi organizace podporující a organizující různé kurzy či semináře o internetové bezpečnosti patří například „Kraje pro bezpečný internet“. Jedná se o projekt poskytující online e-learningové kurzy pro děti, učitele, policisty, rodiče ale i seniory nebo sociální pracovníky.[69] Dalším takovým projektem je „internetem bezpečně“, jehož cílem je pomocí různých vzdělávacích akcí zvýšení povědomí o bezpečnostních rizicích, které mohou na uživatele v kyberprostoru čekat a jak se proti nim bránit.[70] V neposlední řadě je důležité zmínit projekt „E-bezpečí“. „*Projekt E-Bezpečí je celorepublikový certifikovaný projekt zaměřený na prevenci,*

---

[68] POKORNÝ, Pavel. Kyberkriminalita [online]. Zlín, 2016. Diplomová práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky. Vedoucí práce doc. Ing. Martin Sysel, Ph.D. [cit. 2022-08-11]. Dostupné z: http://digilib.k.utb.cz/bitstream/handle/10563/38307/pokorn%C3%BD_2016_dp.pdf?sequence=1&isAllowed=y.

[69] Kraje pro bezpečný internet: Vše o projektu [online]. [cit. 2022-08-07]. Dostupné z: https://www.kpbi.cz/o-projektu

[70] Internetem bezpečně: *O projektu* [online]. [cit. 2022-08-06]. Dostupné z: https://www.internetembezpecne.cz/o-projektu/

vzdělávání, výzkum, intervenci a osvětu spojenou rizikovým chováním na internetu a souvisejícími fenomény.“ Specializací tohoto projektu jsou primárně útoky spočívající v šíření škodlivého obsahu, jako je sexting, kybergrooming, kyberstalking a další. [71]

5. Legislativa spojena s kyberkriminalitou

Pro úspěšný boj s kybernetickou trestnou činností je stejně jako boj s jakoukoliv jinou kriminalitou nutné podpořit kvalitní legislativou na vnitrostátní i mezinárodní úrovni.

5.1. Legislativa v ČR

V rámci České republiky je předpisů, které se váží ke kybernetické kriminalitě hned několik.

5.1.1. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů.

Tento zákon je jednou z nejmladších právních úprav týkajících se kybernetické kriminality a je, jak z názvu vyplývá, zaměřen na kybernetickou bezpečnost.

Předmět úpravy podle §1

> **(1)** *Tento zákon upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti.*
>
> **(2)** *Tento zákon zapracovává příslušné předpisy Evropské unie[6)] a upravuje zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů.*
>
> **(3)** *Tento zákon se nevztahuje na informační nebo komunikační systémy, které nakládají s utajovanými informacemi.*[72]

Tento zákon byl později upraven zákonem č. 205/2017 Sb., *Zákon, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně*

---

[71] E-bezpečí: Informace o projektu [online]. [cit. 2022-08-15]. Dostupné z: https://www.e-bezpeci.cz/index.php/o-projektu/oprojektu

[72] *Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů* [online]. [cit. 2022-15-02]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony.[73]

5.1.2. Trestní zákoník

V rovině represe kybernetické kriminality nelze opomenout zákon č. 40/2009 Sb., Trestní zákoník, který ve své zvláštní části upravuje hned několik právních úprav vztahující se přímo ke kybernetické kriminalitě. Některými z nich jsou:

- §180 Neoprávněné nakládaní s osobními údaji
- §184 Pomluva
- §191 Šíření pornografie
- §192 Výroba a jiné nakládání s dětskou pornografií
- §230 Neoprávněný přístup k počítačovému systému
- §231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat
- §234 Neoprávněné opatření, padělání a pozměnění platebního prostředku
- §270 Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi
- §287 Šíření toxikomanie
- §311 Teroristický útok
- §348 Padělání a pozměnění veřejné listiny
- §355 Hanobení národa, rasy, etnické nebo jiné skupiny osob
- §356 Podněcování nenávisti vůči skupině osob nebo k omezování práv a svobod
- §357 Šíření poplašné zprávy

[74]

---

[73] *Zákon, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony* [online]. [cit. 2022-15-02]. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-205

[74] *Trestní zákoník* [online]. [cit. 2022-02-08]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

5.1.3. Zákoník práce

Zákoník práce je také využívaným dokumentem například v rámci prevence kybernetické kriminality lze uplatnit předpisy dle §316 zákona č. 262/2006 Sb., Zákoník práce, ve znění:

> **(1)** *Zaměstnanci nesmějí bez souhlasu zaměstnavatele užívat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky ani jeho telekomunikační zařízení. Dodržování zákazu podle věty první je zaměstnavatel oprávněn přiměřeným způsobem kontrolovat.*
>
> **(2)** *Zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci.*
>
> **(3)** *Jestliže je u zaměstnavatele dán závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele, který odůvodňuje zavedení kontrolních mechanismů podle odstavce 2, je zaměstnavatel povinen přímo informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění.*

Tímto předpisem je tedy povolen monitoring zaměstnanců, pakliže jsou o něm zaměstnanci dostatečně informováni. (viz. kapitola 5.1.3. této práce) Bez této právní úpravy by mohl být považován monitoring za neoprávněné narušení soukromí. [75]

5.1.4. NBU

Národní bezpečnostní úřad je orgánem výkonné moci, zřízený na základě zákona č. 148/1998 sb., zákon o ochraně utajovaných skutečností.

„Podle usnesení vlády České republiky ze dne 19. října 2011 č. 781 je gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast NBÚ. Organizační řešení potřeby centralizovaného vyhodnocování

---

[75] *Zákoník práce* [online]. [cit. 2022-11-02]. Dostupné z: https://www.zakonyprolidi.cz/cs/2006-262

informací o kybernetické bezpečnostní situaci České republiky bude postaveno na existenci dvou dohledových pracovišť, tj. vládního CERT/CSIRT a národního CERT/CSIRT“ [76]

5.1.4.1. NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost je ústřední správní orgán pro kybernetickou bezpečnost. Výkonnou sekcí úřadu je Národní centrum kybernetické bezpečnosti (NCKB). NCKB zajišťuje zejména:

- činnost Vládního CERT České republiky (GovCERT.CZ), -
- prevenci před kybernetickými hrozbami proti prvkům kritické informační infrastruktury
- řešení a koordinaci řešení kybernetických bezpečnostních incidentů u subjektů kritické infrastruktury,
- provozovatelů základní služby a orgánů veřejné správy osvětovou a vzdělávací činnost v oblasti kybernetické bezpečnosti
- spolupráci s národními i mezinárodními organizacemi podílejícími se na zajišťování bezpečnosti kybernetického prostoru
- pořádání a účast na kybernetických cvičeních na národní a mezinárodní úrovni
- výzkum a vývoj v oblasti kybernetické bezpečnosti[77]

5.1.4.2. Vládní CERT

Tým CERT (Computer emergency response team) je zásadním úsekem při ochraně kritické informační infrastruktury dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Vzhledem k faktu, že čím dál tím více zemí má připojené své kritické systémy připojeny k internetu je nutné, aby stát přijal veškerá nezbytná opatření k jejich ochraně a pokud již dojde k selhaní preventivních

---

[76] *Věcný záměr zákona o kybernetické bezpečnosti* [online]. [cit. 2022-25-02]. Dostupné z: https://www.vlada.cz/assets/ppov/lrv/ria/databaze/Vecny-zamer-zakona-o-kyberneticke-bezpecnosti.doc

[77] *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2022-01-18]. Dostupné z: https://www.nukib.cz/cs/o-nukib/

opatření je nezbytné mít tým jako je CERT, který je schopný rychle a účelně reagovat na napadení infrastruktury.

Zároveň týmy CERT hrají důležitou roli v rámci zvyšování povědomí a vzdělanosti ohledně bezpečnosti na internetu.[78]

5.1.4.3. CSIRT.CZ

Tým CSIRT.CZ (Computer security incident response team) je českým uskupením v rámci mezinárodních týmů CSIRT po celém světě. Na rozdíl od Vládního CERT týmu, CSIRT.CZ má za úkol asistovat a spolupracovat se subjekty provozující počítačové sítě v rámci České republiky. Subjekty v gesci CSIRT.CZ týmu jsou ISP, poskytovatelé služeb, banky, bezpečnostní složky, úřady státní správy a jiné instituce.

Dalším důležitým úkolem je udržování mezinárodních vztahů mezi jednotlivými týmy typu CSIRT, neboť častokrát páchaná kyberkriminalita překračuje hranice států mezinárodní kooperace nevyhnutelná a zároveň výhodná pro všechny.[79]

5.2. Mezinárodní úmluvy

V rámci mezinárodních úmluv jsou v rámci Evropské Unie asi dva nejdůležitější dokumenty a těmi jsou „Úmluva rady Evropy o kybernetické kriminalitě“ a dodatkový protokol k úmluvě o kybernetické kriminalitě a spolu s nimi přispívají k ochraně před kyberkriminalitou další Sdělení Evropské unie.

5.2.1. Úmluva Rady Evropy č.185 o kybernetické kriminalitě a její dodatek

Jedná se o první mezinárodní dohodu jejíž předmětem úpravy je kriminality páchána v kyberprostoru. V Úmluvě je nejdříve definováno v kapitole 1, co je počítačový systém a data, kdo je poskytovatel služby a co jsou to provozní data.

Dále Úmluva v kapitole 2 časti první, jmenuje opatření, která musí být v rámci trestního práva hmotného na vnitrostátní úrovní přijata. Rozdělena je do 5

---

[78] Národní úřad pro kybernetickou a informační bezpečnost: *Vládní CERT* [online]. [cit. 2022-01-20]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/vladni-cert/

[79] CSIRT.CZ: *O nás* [online]. [cit. 2022-07-21]. Dostupné z: https://csirt.cz/cs/o-nas/

oddílů z nichž 4 oddíly popisují skutkové podstaty kybernetických trestných činů a oddíl 5 upravuje odpovědnosti a tresty.

Oddíl 1 – Trestné činy proti utajování, integritě a dostupnosti počítačových dat a systémů

Oddíl 2 – Trestné činy související s počítači

Oddíl 3 – Trestné činy související s obsahem

Oddíl 4 – Trestné činy související s porušováním autorských práv a práv souvisejících

Oddíl 5 – Další formy odpovědnosti a trestů

Úmluva v kapitole 2 části druhé upravuje opatření tentokráte trestního práva procesního, které musí být přijaty na vnitrostátní úrovni. V kapitole 3 je pak rozebrána mezinárodní spolupráce a její zvláštní ustanovení a v kapitole 4 se nachází závěrečná ustanovení. [80]

V dodatku jsou pak doplněny znaky skutkových podstat, které v původní Úmluvě rozepsány nebyly a těmi jsou trestné činy související s šířením rasistického a xenofobního materiálu.

Těmito materiály se pak rozumí dle dodatku rozumí – „…*jakýkoli písemný materiál, obraz nebo jiné vyjádření myšlenek nebo teorií, který obhajuje, podporuje nebo podněcuje nenávist, diskriminaci nebo násilí, proti jakémukoli jednotlivci nebo skupině jednotlivců, na základě rasy, barvy pleti, rodového nebo národního nebo etnického původu, jakož i náboženství, pokud je použito jako záminka namísto nějakého z těchto atributů*“ [81]

Tato Úmluva byla podepsána jménem České republiky 9.2.2005, a pro Českou republiku vstoupila úmluva v platnost podle odstavce 4 článku 36 dne 1. prosince 2013.

---

[80] *Úmluva Rady Evropy č.185 o kybernetické kriminalitě ze dne 23.11.2001* [online]. Dostupné z: https://www.zakonyprolidi.cz/ms/2013-104/zneni-20190705

[81] *Dodatkový protokol k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů* [online]. [cit. 2022-07-05]. Dostupné z: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804931bf

5.2.2. Další mezinárodní dokumenty

Sdělení Komise Evropskému Parlamentu, Radě, Evropskému Hospodářskému a Sociálnímu Výboru a Výboru Regionů boj proti spamu a špionážnímu („spyware“) a škodlivému softwaru („malicious software“) ze dne 15.11.2006

„Toto sdělení se zabývá vývojem v oblasti spamu a hrozbami, jako jsou špionážní software (dále jen „spyware“) a škodlivý software. Hodnotí úsilí, které bylo doposud vynaloženo v boji s těmito hrozbami, a určuje další opatření, která mohou být přijata“ [82]

Sdělení komise Evropskému parlamentu, Radě a Evropskému Výboru regionů – k obecné politice v boji proti počítačové kriminalitě. Cílem tohoto sdělení je: *„zdokonalit a usnadnit koordinaci a spolupráci mezi jednotkami boje proti počítačové kriminalitě, dalšími příslušnými orgány a odborníky v Evropské unii - v koordinaci s členskými státy, příslušnými organizacemi EU a mezinárodními organizacemi a dalšími zúčastněnými stranami vypracovat ucelený politický rámec EU v boji proti počítačové kriminalitě - zlepšit obecné povědomí o nákladech a nebezpečích vyplývajících z počítačové kriminality“* [83]

Další dokumenty napomáhající k ochraně před kyberkriminalitou vydává i Rada spojených národů OSN, primárně potírající nejen kybernetické formy terorismu v rámci členských států.

6. Statistika kybernetické kriminality za roky 2011-2020

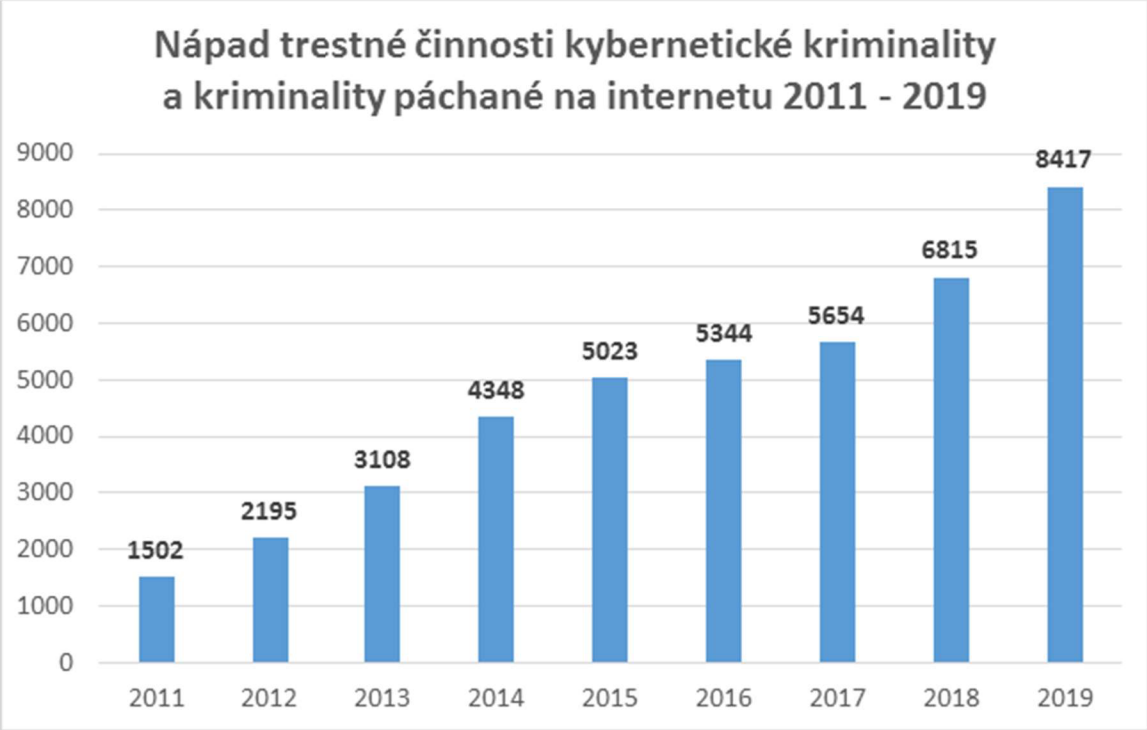
Při pohledu na statistický graf trestné činnosti kybernetické kriminality a kriminality na internetu v letech 2011-2019 je vidět, že v těchto letech docházelo k setrvalému nárustu kybernetické kriminality, jehož příčinou je rostoucí trend informačních technologií a jeho neustálá dynamika spojena s vývojem nových technologií. Policie ČR uvádí, že v roce 2019: „*Tradičně nejpočetnější skupinou v*

---

[82] Sdělení komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů boj proti spamu a špionážnímu („spyware“) a škodlivému softwaru („malicious software“) [online]. [cit. 2022-07-20]. Dostupné z: https://eur-lex.europa.eu/legal-content/cs/TXT/?uri=CELEX:52006DC0688 („malicious software“) [online]. Dostupné z: https://eur-lex.europa.eu/legal-content/cs/TXT/?uri=CELEX:52006DC0688

[83] Sdělení komise Evropskému parlamentu, Radě a Evropskému Výboru regionů – k obecné politice v boji proti počítačové kriminalitě [online]. [cit. 2022-07-20]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52007DC0267

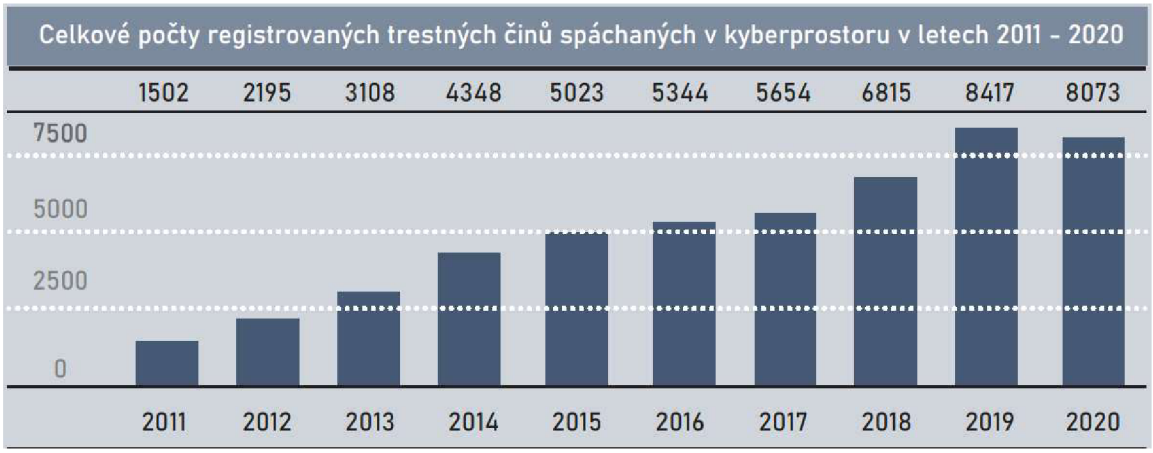
oblasti kybernetické kriminality a kriminality páchané na internetu jsou různé formy podvodného jednání (více než polovina všech evidovaných skutků), vedle kterých jsou nemalou měrou zastoupeny i pojistné podvody. Téměř o třetinu vzrostl počet případů tzv. hackingu (na 930), což jsou zejména případy neoprávněného přístupu k počítačovému systému a nosiči informací. Významné zastoupení má stále také mravnostní kriminalita (777 skutků).“ [84]



Příloha č.1 – Graf nápadu trestné činnosti kybernetické kriminality 2011-2019

V letech 2019-2020 evidujeme mírný pokles o necelých 5 %, který je pravděpodobně zapříčiněn legislativní změnou trestního zákoníku, která zvýšila hranice výše škody pro kvalifikaci trestného činu. Tedy podvody menšího rozsahu se do trestných činů nezapočítaly. Bohužel v době psaní této práce nejsou ještě k dispozici statistická data za rok 2021 takže je nelze srovnat s lety předchozími.

[84]Policie ČR: Kyberkriminalita [online]. [cit. 2022-06-09]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx



Příloha č.2 – Graf nápadu trestné činnosti kybernetické kriminality 2011-2020

Závěr

Společně s vývojem informačních technologií vzrostl počet případů, kdy byly tyto technologie zneužity k trestné činnosti. V rámci protizákonných aktivit je tak nutné řešit i případy, které jsou v současné době obsaženy v termínu „kybernetická kriminalita“.

Do pojmu kybernetická kriminalita je zahrnuto mnoho kybernetických útoků, Mezi ty snadnější můžeme zahrnout, internetové podvody, šíření fake news, nelegální obchodování s drogami nebo s kradenými díly chráněnými zákonem. Komplikovanější kriminalita je pak užití spyware, DDoS útoků na specifické systémy, útoky sociálního inženýrství tedy phishing a pharming, rootkiting, anebo různé typy malware transportované trojskými koňmi. Ať už kriminalita kybernetická nebo ne, nevyhne se kyberprostoru ani kriminalita mravnostní. S jednoduchostí používaní internetu je snadné šířit dětskou či jinou pornografii. Kyberstalking a kybergrooming jsou s pomocí internetu také poměrně snadno realizovatelné. Na internetu se mimo jiné sdružují i nebezpečné potencionálně extremistické skupiny či hackeři teroristických skupin.

Vzhledem k téměř každodennímu využívání informačních technologií je určitému riziku hackerského útoku vystaven každý. V rámci tzv. kyberprostoru je složitější odhalit identitu jednotlivých uživatelů, tudíž je i snazší pro pachatele uniknout případnému odhalení. V reakci na kybernetická nebezpečí je tedy důležité rozšířit si znalosti o možnosti ochrany proti nim. V dnešní době je dobré zainvestovat do, jak se útokům bránit, ať už se chce chránit osoba fyzická či právnická.

Seznam použité literatury

Monografie

GŘIVNA, Tomáš, SCHEINOST, Miroslav a ZOUBKOVÁ, Ivana. *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. s. 390-407 ISBN 978-80-7598-554-5.

KOLOUCH, Jan a VOLEVECKÝ, Petr. *Trestněprávní ochrana před kybernetickou kriminalitou.* Praha: Policejní akademie České republiky v Praze, 2013. ISBN 978-80-7251-402-1.

KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. s. 74-148. ISBN 978-80-88168-15-7.

KREMLING, Janine a PARKER, Amanda M. S. Cyberspace, cybersecurity, and cybercrime. London; Washington DC; New Delhi; Los Angeles; Singapore; Melbourne; SAGE, 2018. s. 50-51. ISBN 978-15-06347-25-7;

MARAS, Marie-Helen. Cybercriminology. New York; Oxford; Oxford University Press, 2017. s. 3-5. ISBN 978-01-90278-44-1;

ZAVRŠNIK, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7552-758-5.

Online přístupné zdroje

BLANTON, Sean. *„What is user management?“* [online]. [cit. 2021-10-02]. Dostupné z: https://jumpcloud.com/blog/what-is-user-management

CSIRT.CZ: *O nás* [online]. [cit. 2022-07-21]. Dostupné z: https://csirt.cz/cs/o-nas/

DENNING, Dorothy E. *Definice pojmu kyberterorismus* [online]. [cit. 2021-01-16]. Dostupné z: https://fas.org/irp/congress/2000_hr/00-05-23denning.htm

E-bezpečí: *Informace o projektu* [online]. [cit. 2022-08-15]. Dostupné z: https://www.e-bezpeci.cz/index.php/o-projektu/oprojektu

Finanční vzdělávání: *Praní špinavých peněz*. [online]. [cit. 2022-08-15]. Dostupné z: https://www.financnivzdelavani.cz/svet-financi/bankovnictvi/prani-spinavych-penez

GREBENNIKOV, Nikolay. *„Keyloggers: How they work and how to detect them (Part 1)“.* [online]. [cit. 2022-01-22]. Dostupné z: https://securelist.com/keyloggers-how-they-work-and-how-to-detect-them-part-1/36138/

Internetem bezpečně: *Kybergrooming* [online]. [cit. 2022-08-06]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybergrooming/

Internetem bezpečně: *Kyberstalking* [online]. [cit. 2022-08-06]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kyberstalking/

Internetem bezpečně: *O projektu* [online]. [cit. 2022-08-06]. Dostupné z: https://www.internetembezpecne.cz/o-projektu/

JOHANSEN, Alison Grace. *„What is a firewall? Firewalls explained and why you need one.“* [online]. [cit. 2021-06-17]. Dostupné z: https://us.norton.com/internetsecurity-emerging-threats-what-is-firewall.html

JOHANSEN, Alison Grace. *„What is antivirus software? Antivirus definition.“* [online]. [cit. 2019-02-22]. Dostupné z: https://us.norton.com/internetsecurity-emerging-threats-what-is-firewall.html

Irwin, Angela & Slay, Jill. (2012). Detecting Money Laundering and Terrorism Financing Activity in Second Life and World of Warcraft. International Cyber Resilience conference. [online] Dostupné z: https://www.researchgate.net/publication/49285565_Detecting_Money_Laundering_and_Terrorism_Financing_Activity_in_Second_Life_and_World_of_Warcraft

KAPOOR, Aditya a SALLAM, Ahmed. Rootkits Part 1 of 3: *The Growing Threat*. [online]. [cit. 2022-01-22]. Dostupné z: http://download.nai.com/Products/mcafee-avert/whitepapers/akapoor_rootkits1.pdf

KAPOOR, Aditya a SALLAM, Ahmed. Rootkits Part 2 of 3: *A Technical Primer*. [online]. [cit. 2022-01-22]. Dostupné z: https://www.01net.it/wp-content/uploads/sites/14/2014/10/McAfee_rootkit_windows.pdf

Kaspersky: *What is data encryption?* [online]. [cit. 2022-07-22]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/encryption

Kaspersky: *What is Pharming and how to protect yourself* [online]. [cit. 2022-07-22]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/pharming

Kaspersky: *What is a Computer Virus or a Computer Worm?* [online]. [cit. 2022-02-04]. Dostupné z: https://www.kaspersky.co.uk/resource-center/threats/viruses-worms

KOVALČÍK, Marek. *Etický hacking – laicky a jednoduše: Tři typy hackerů.* BDO [online]. 2020. Dostupné z: https://www.bdo.cz/cs-cz/archiv/it-security/12-2020/eticky-hacking-%E2%80%93-laicky-a-jednoduse

Kraje pro bezpečný internet: *Vše o projektu* [online]. [cit. 2022-08-07]. Dostupné z: https://www.kpbi.cz/o-projektu

LASKOW, Sarah. *"The Counterintuitive History of Black Hats, White Hats, And Villains"* [online]. 2017. [cit. 2022-01-19]. Dostupné z: https://www.atlasobscura.com/articles/the-counterintuitive-history-of-black-hats-white-hats-and-villains

MARKS, Jonathan T. *„Cryptocurrency and money laundering: why understanding fraud is critical“* [online]. [cit. 2021-11-15]. Dostupné z: https://www.bakertilly.com/insights/cryptocurrency-and-money-laundering

MIKHAYLOVA, Galina. *Definice pojmu hacktivismus* [online]. 2014. [cit. 2022-01-19]. Dostupné z: https://digital.library.txstate.edu/bitstream/handle/10877/5378/MIKHAYLOVA-THESIS-2014.pdf?sequence=1

Ministerstvo vnitra České republiky MV ČR: Definice pojmu terorismus [online]. [cit. 2022-01-16]. Dostupné z: https://www.mvcr.cz/clanek/definice-pojmu-terorismus.aspx

Národní úřad pro kybernetickou a informační bezpečnost [online]. [cit. 2022-01-18]. Dostupné z: https://www.nukib.cz/cs/o-nukib/

Národní úřad pro kybernetickou a informační bezpečnost: *Vládní CERT* [online]. [cit. 2022-01-20]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/vladni-cert/

National cybersecurity alliance: *„Back it up“* [online]. [cit. 2021-01-20]. Dostupné z: https://staysafeonline.org/stay-safe-online/online-safety-basics/back-it-up/

Novinky.cz: *Tvrdý trest za schvalování terorismu na internetu. Muž dostal šest let vězení* [online]. [cit. 2021-03-16, v čase 15:07]. Dostupné z: https://www.novinky.cz/krimi/clanek/tvrdy-trest-za-schvalovani-terorismu-na-internetu-muz-dostal-sest-let-vezeni-40354135

POKORNÝ, Pavel. *Kyberkriminalita* [online]. Zlín, 2016. Diplomová práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky. Vedoucí práce doc. Ing. Martin Sysel, Ph.D. [cit. 2022-08-11]. Dostupné z: http://digilib.k.utb.cz/bitstream/handle/10563/38307/pokorn%C3%BD_2016_dp.pdf?sequence=1&isAllowed=y.

Policie ČR: *Hlášení kyberkriminality* [online]. [cit. 2022-06-09]. Dostupné z: https://www.policie.cz/clanek/hlaseni-kyberkriminality.aspx

Policie ČR: *Kyberkriminalita* [online]. [cit. 2022-06-09]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

ROSENCRANCE, Linda. *Software* [online]. [cit. 2022-07-12]. Dostupné z: https://www.techtarget.com/searchapparchitecture/definition/software

Sentient digital, inc.: *„What is cyber monitoring?“* [online]. [cit. 2021-10-05]. Dostupné z: https://sdi.ai/blog/what-is-cyber-monitoring/

SMEJKAL, Vladimír. *Kybernetická kriminalita.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. Pro praxi. ISBN 978-80-7380-501-2.

Spyware Workshop: *Monitoring Software On Your Personal Computer: Spyware, Adware, and Other Software: Report of the Federal Trade Commission Staff".* [online]. [cit. 2022-07-25]. Dostupné z: https://www.ftc.gov/reports/spyware-workshop-monitoring-software-your-personal-computer-spyware-adware-other-software

Stanford University: *What is hacktivism* [online]. [cit. 2022-01-17]. Dostupné z: https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/Hacktivism/what.html

Techslang: Torrenting: What is It and How does It Work? [online]. [cit. 2022-02-09]. Dostupné z: https://www.techslang.com/torrenting-what-is-it-and-how-does-it-work/

Dodatkový protokol k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů [online]. [cit. 2022-07-05]. Dostupné z: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804931bf

Legislativní zdroje

Kapitola II., články 3,4,5,6, Dodatkového protokol k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů.

Trestní zákoník [online]. [cit. 2022-02-08]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

Sdělení komise Evropskému parlamentu, Radě a Evropskému Výboru regionů – k obecné politice v boji proti počítačové kriminalitě [online]. [cit. 2022-07-20]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52007DC0267

Sdělení komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů boj proti spamu a špionážnímu („spyware") a

škodlivému softwaru („malicious software“) [online]. [cit. 2022-07-20]. Dostupné z: https://eur-lex.europa.eu/legal-content/cs/TXT/?uri=CELEX:52006DC0688

Úmluva Rady Evropy č.185 o kybernetické kriminalitě ze dne 23.11.2001 [online]. Dostupné z: https://www.zakonyprolidi.cz/ms/2013-104/zneni-20190705

Věcný záměr zákona o kybernetické bezpečnosti [online]. [cit. 2022-25-02]. Dostupné z: https://www.vlada.cz/assets/ppov/lrv/ria/databaze/Vecny-zamer-zakona-o-kyberneticke-bezpecnosti.doc

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů [online]. [cit. 2022-15-02]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

Zákon o právu autorském [online]. [cit. 2022-20-02]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-121

Zákon, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony [online]. [cit. 2022-15-02]. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-205

Zákoník práce [online]. [cit. 2022-11-02]. Dostupné z: https://www.zakonyprolidi.cz/cs/2006-262