DETEKCE A PREVENCE KYBERNETICKÝCH HROZEB

Za tuto publikaci odpovídá pouze její autor. Evropská unie nenese odpovednost za jakékoli využití informací v ní obsažených.

Co-funded by the Erasmus+ Programme of the European Union

Obsah

1. Úvod

V současné době se není možné oprostit od informačních a komunikačních technologií. Přínos těchto technologií pro společnost ve všech oblastech lidské činnosti (např. v lékařské vědě, výzkumné činnosti, bezpečnosti, dopravě aj.) je neoddiskutovatelný. Oblast informačních a komunikačních technologií je nejrychleji a nejvíce se rozvíjejícím odvětvím lidské činnosti.

To, co je třeba si uvědomit, je skutečnost, že informace či data a jejich využití v sobě zahrnují značný ekonomický i politický potenciál. Informace a jejich obsah mohou rozhodovat nejen o bytí či nebytí jednotlivce či firmy, ale ve své podstatě jsou schopny ovlivnit celosvětový vývoj.

Využití informačních a komunikačních technologií má však i stinné stránky. Jednou z nich je bezesporu i gigantický a dynamický nárůst „nového druhu" trestné činnosti, se kterou je třeba se vypořádat tak, aby nedocházelo k ohrožování a porušování zájmů společnosti. Tuto trestnou činnost lze souhrnně nazvat kyberkriminalitou.[1]

Je třeba zmínit, že v celosvětovém měřítku lze pozorovat značnou snahu jak na právní, tak i bezpečnostní úrovni, jejímž cílem je přijmout adekvátní opatření, která by byla schopna reagovat na tento nový a dynamický fenomén současnosti.[2]

Klíčovými body pro rozvoj kyberkriminality se staly tři skutečnosti.[3] První z nich je propojení čtyř univerzitních počítačů a vytvoření počítačové sítě určené ke sdílení dat.[4] Druhým pak vytvoření prvního osobního počítače (PC - Personal Computer) společností IBM na konci 80. let 20. století. Třetím a dle mého názoru nejvýznamnějším milníkem pak je zpřístupnění Internetu široké veřejnosti, včetně úpravy jednotlivých aplikací do uživatelsky přívětivější podoby.

Rozvoj současné digitální společnosti není založen přímo na hospodářském rozvoji spojeném s hmotnými zdroji, ale na rozvoji IT, na připojování stále většího počtu uživatelů do Internetu, ale zejména k aplikacím jako takovým a v neposlední řadě na zisku informací a dat od uživatelů samotných. Tyto změny související s rozvojem IT probíhajícím jak v sociální, tak i ekonomické rovině a jsou jednou z příčin kyberkriminality.

Kyberprostor je v současnosti nejúčinnější a nejnebezpečnější zbraní v rukou pachatelů kybernetické trestné činnosti. Nejde o to, že by byl kyberprostor, či Internet sám o sobě nebezpečný, či nezabezpečený. Podstatou je, že systém je vždy tak silný, jak je silný jeho nejslabší článek. V tomto případě je tím nejslabším prvkem, víc než kdy jindy, uživatel. Uživatel je vlastně sám sobě a svému okolí největší „hrozbou", protože byť má právní subjektivitu[5], tak často má jen minimální znalosti o svých právech a povinnostech.

Internet se stal součástí našeho každodenního života a zejména jeho multimediální aspekt se velmi rychle rozvíjí. Internet je, ať chceme či nechceme, silnějším a dravějším médiem než televize či jakékoli jiné masmédium. Už nyní může dokonce i prostý uživatel prostřednictvím jednoduchého rozhraní předat či vnutit celé světové populaci svou myšlenku, názory. A je jedno, zda jsou to myšlenky normální, či jakkoli zvrácené.

Na jedné straně Internet nabízí prakticky neomezené možnosti téměř komukoli v získávání a zpracovávání informací téměř o čemkoli, bez nutnosti trávení času v knihovnách či informačních centrech mimo domov (získání předmětných informací je otázkou několika vteřin).

Google a Wikipedia se staly relevantním a mnohdy jediným zdrojem informací pro naše rozhodnutí. Internet umožňuje komunikaci sbližující lidi mezi sebou navzájem, usnadňuje řadu aktivit díky možnosti nalezení řešení či návodu, nabízí množství různých informačních kanálů aj. Přitom to vše umožňuje dělat z prostředí domova a s pocitem téměř absolutní anonymity.

Na druhé straně může mít činnost v tomto virtuálním prostředí za následek těžké finanční ztráty, strach ze zásahů do svého soukromí cizími osobami, ztrátu cenných osobních dat, online komunikaci psychicky narušených osob (pedofilů, drogově závislých, filozoficky dezorientovaných apod.), komunikaci těchto osob s našimi vlastními dětmi za našimi zády, domlouvání kriminálních skupin na nezákonné činnosti bez možnosti odposlechu třetí stranou, podvody, neautorizované průniky do soukromých sfér firem, přesměrovávání obchodních zakázek, vykrádání cizích účtů, ničení dat a databází, poškozování autorského práva atd.

Nelze připustit, aby se kyberprostor stal prostředím, kde by pachatelé mohli páchat de facto beztrestně jakoukoliv trestnou činnost. Existuje ale pouze jeden výchozí bod pro boj proti kriminalitě v kyberprostoru, a tím je kyberprostor sám. Je třeba pochopit, co vlastně kyberprostor představuje, na jakých principech pracuje, jaké typy kriminality se mohou v tomto virtuálním světě vyskytovat a co vše mohou orgány činné v trestním řízení, ale zejména uživatel sám, proti této protiprávní činnosti dělat.

Jak již bylo řečeno, kyberkriminalita nabývá v poslední době na stále větší intenzitě. Díky její různorodosti dochází k zásahům do široké škály základních lidských práv každého z nás a informační a komunikační technologie se tak stávají prostředky, jimiž dochází k páchání trestné činnosti nebo jsou samy cílem této činnosti.

Výraznou odlišností kybernetické kriminality od ostatních druhů kriminality je její značná latentnost, mnohdy vysoká míra tolerance společností (včetně lhostejnosti uživatelů k případným hrozbám), reálná či domnělá anonymita pachatele a jeho obtížná identifikace, jakož i celý proces dokazování. Proto je třeba řešit nejen otázky represivního působení na pachatele, ale je třeba se zabývat také otázkou prevence trestné činnosti v této oblasti, jakož i otázkou možné ochrany společnosti před touto trestnou činností.

Vlastní prevence zmíněných negativních jevů musí nutně začít u koncových uživatelů, neboť v kyberprostoru jsou to právě oni, kdo je typickou první obětí útočníka. Na základě svých zkušeností jsem pevně přesvědčen o tom, že výchova a vzdělávání uživatelů má být nezbytnou součástí prostupu informačních a komunikačních technologií do našich životů. Myslím si, že budování informační gramotnosti by mělo být neodmyslitelně spojeno s tvorbou, distribucí a podporou produktů či služeb, které jsou s informačními a komunikačními technologiemi spojeny. Vlastní vzdělávání v této oblasti, či spíše seznamování se s možnými hrozbami, riziky a negativy IT, by mělo být součástí výuky všech forem studia na všech úrovních školství.

Pokud se jedná o osoby, které se této problematice věnují v rámci své profese, pak jsou na tyto specialisty kladeny ještě vyšší nároky, neboť se musí neustále zdokonalovat a školit, aby byli schopni čelit stále novým a dynamicky narůstajícím útokům páchaným prostředky a v prostředí ICT.

[1] **Kyberkriminalita** je mnohdy označována různými názvy. Domnívám se, že nejvýstižnějším pojmem, označujícím toto protiprávní jednání, je právě pojem kyberkriminalita. V této monografii budou pro označení tohoto jevu používány i pojmy **kyberkriminalita, kybernetická kriminalita či kybernertická trestná činnost**.

Pokud bychom vycházeli z doslovného překladu anglického názvu **Cybercrime**, pak překlad kyberkriminalita není přesný, neboť doslovný překlad tohoto spojení dvou slov je možné přeložit jako: **kyber zločin** (případně **trestný čin**). Avšak i v prostředí České republiky je vžit a běžně užíván překlad **Convention on Cybercrime**, jako **Úmluva o Kyberkriminalitě**, byť tento překlad není, jak je uvedeno výše, doslovný. Domnívám se proto, že i vzhledem k tomuto překladu není pochybením užívání pojmu kyberkriminalita.

Vymezení rozdílů mezi kriminalitou a trestnou činností na tomto úseku bude obsaženo v další části této publikace, stejně jako vymezení názorů různých autorů na přesné označení této trestné činnosti. V publikaci budou jako synonyma využívány zejména pojmy kybernetická trestná činnost a kyberkriminalita.

[2] Např: *Fight against cyber crime: cyber patrols and Internet investigation teams to reinforce the EU strategy.* [online]. [cit.10.7.2016]. Dostupné z: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1827

[3] Tyto skutečnosti pak byly podpořeny řadou dalších okolností (např. nedostatek právní úpravy ve vztahu k Internetu, neschopností vynutit právo, pocitem anonymity uživatelů aj.).

[4] Blíže viz ARPANET či NSFNET. Jedná se o období konce 60. let 20. století.

Srov. *Historical Maps of Computer Networks*. [online]. [cit.10.7.2016]. Dostupné z:

https://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/historical.html

[5] Mají práva a povinnosti. Uživatelé zakládají, mění a případně ruší právní vztahy.

2. Pojem kybernetické trestné činnosti a pojmy související

- Cybercrime
- Klasifikace forem kyberkriminality
- Kybernetický útok (Cyber attack)

2.1. Cybercrime

Užívání výpočetní techniky, informačních systémů a informačních technologií a jejich integrace do téměř všech odvětví lidské činnosti je jevem, který je pro dnešní dobu charakteristický. Lze konstatovat, že **v podstatě nejde nalézt takovou oblast lidské činnosti, kde by se přímo nebo zprostředkovaně nevyužívala výpočetní technika, resp. informační systém nebo informační či komunikační technologie**.

Bohužel, tak jak rostou možnosti užívání těchto vymožeností dnešní doby a vědeckotechnického pokroku, rostou i možnosti a zároveň i četnost jejich zneužívání k páchání páchání trestné činnosti.

V 90. letech 20. století se pro trestnou činnost páchanou pomocí informační techniky ustálil pojem **„počítačová kriminalita“** (*Computercrime*, *Computerkriminalität*). Smejkal ve své publikaci definuje, v polovině 90. let 20. století, *počítačovou kriminalitu*, jako různorodou směsici trestných činů, jejichž společným faktorem je počítač, program a data. Pod pojmem počítačová kriminalita *„…je třeba chápat páchání trestné činnosti, v níž figuruje počítač jako souhrn hardwarového a softwarového vybavení data nevyjímaje, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět této trestné činnosti, ovšem **s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako movité věci, nebo jako nástroje trestné činnosti.**“*[1] Z uvedené definice je patrné, že počítačová kriminalita se vztahovala pouze na počítačové systémy, jakožto na cíle útoku.

Označení „počítačová kriminalita“ evokuje představu, že trestný čin musí být spáchán na počítači nebo prostřednictvím počítače, nejčastěji počítače osobního (PC - Personal Computer). Takové chápání je dnes zjednodušující, zároveň i poněkud kvantitativně redukuje množství jevů, které lze pod pojem trestná činnost páchaná prostředky informačních a komunikačních technologií zahrnout. Mnohá technická zařízení v dnešní době, díky implementaci mikroprocesorů spolu s jejich miniaturizací, již dávno převzala funkci osobních počítačů (PC), aniž by byla sama za osobní počítače označována. Jedná se o hybridy plnící rozličné funkce, které dříve plnily speciální přístroje. Soudobá technická zařízení umožňující komunikaci mezi sebou a mezi jejich uživateli a jejichž konstrukce je vedena myšlenkou *ALL-IN-ONE* (vše v jednom) dosahují mnohem větších výpočetních výkonů, než nejmodernější výpočetní jednotky z první poloviny 90. let. A i tyto prostředky[2], přestože nejsou nazývány počítači, mohou být terčem trestné činnosti či prostředkem k jejímu spáchání. Z těchto důvodů se pojem „počítačová kriminalita“ či „počítačový trestný čin“ v dnešní době již v odborné literatuře téměř nepoužívá. Namísto pojmu „počítač“ je v dnešní době používán spíše výraz „informační a komunikační technologie“ (*Information and Communiction Technology – ICT*), resp. „trestné činy v ICT“.[3]

V roce 2000 vydala Rada Evropy definici počítačové kriminality pocházející ze Statutu Komise expertů pro zločin v kyberprostoru: *„Trestný čin namířený proti integritě, dostupnosti nebo utajení počítačových systémů nebo trestný čin v tradičním smyslu, při kterém je užito moderních informačních a komunikačních technologií“*[4]

Rámcové rozhodnutí Rady EU č. 2002/584/JHA o evropském zatýkacím rozkazu označuje za **„computer-related crime“** takové jednání, které směřuje proti počítači, či jednání, kde je počítač prostředkem ke spáchání trestného činu. Ze znění evropského zatýkacího rozkazu pak vychází i definice kyberkriminality.

V mezinárodních úmluvách se pro trestnou činnost páchanou prostředky informačních technologií užívá nejčastěji pojem „**kybernetická kriminalita**“ (*Cyber Crime)* a používání tohoto pojmu se z oblasti normativní přeneslo též do slovníku odborné veřejnosti. Pojem kyberkriminalita má obdobný charakter jako pojmy *„násilná kriminalita“, „kriminalita mladistvých“, „ekonomická kriminalita“ apod. Takovýmito názvy jsou označovány skupiny trestných činů mající určitý společný faktor, jako např. způsob provedení, osobu pachatele (alespoň druhově) apod. Ve své podstatě přitom může jít o velmi různorodou směsici trestných činů, spojených oním společným faktorem (počítačem, programem, daty).*“[5]

Při vymezení obsahu pojmu **kybernetická kriminalita** si je třeba uvědomit, že spolu s růstem možností využívání informačních a komunikačních prostředků roste i možnost jejich užívání (zneužívání) k páchání trestné činnosti. Proto v podstatě neexistuje jakási univerzální, obecně přijímaná definice, která by rozsah a hloubku tohoto pojmu plně postihla.

Jednu z možných definic počítačové či kybernetické kriminality je možné nalézt i ve Výkladovém slovníku kybernetické bezpečnosti[6]:

Cyber crime

„Criminal activity in which a computer appears in some way as an aggregate of hardware and software (including data), or only some of its components may appear, or sometimes a larger number of computers either standalone or interconnected into a computer network appear, and this either as the object of interest of this criminal activity (with the exception of such criminal activity whose objects are the described devices considered as immovable property) or as the environment (object) or as the instrument of criminal activity (See Computer crime).“

Počítačová kriminalita /Kybernetická kriminalita - Computer crime / Cyber crime

„Crime committed using a data processing system or computer network or directly related to them.“

Z těchto dvou definic je patrná snaha o vymezení všech aspektů kybernetické kriminality, avšak autoři se dopustili určitých nepřesností. Zaprvé využívají oba dva uvedené termíny jako synonymum, avšak v definici počítačová kriminalita pomíjí faktory, že počítač je zároveň cílem i prostředkem útoku. Obdobné problémy spojené s vlastním definováním pojmu kybernetická kriminalita je možné nalézt i jinde.

Vzhledem ke snaze o definování pojmu kybernetické kriminality je vhodné využít Úmluvu Rady Evropy č. 185 o kybernetické kriminalitě ze dne 23. listopadu 2001.[7] Tato úmluva však vlastní pojem kyberkriminality nevymezuje. Definuje pouze opatření, která by měla být přijata ratifikující stranou na vnitrostátní úrovni. Tato opatření v oblasti trestního práva hmotného pak vymezují hrubý rámec trestných činů, které jsou považovány za kybernetické trestné činy. Toto rámcové vymezení (spolu s dalšími trestnými činy obsaženými v Dodatkovém protokolu Rady Evropy č. 189 k Úmluvě o kybernetické kriminalitě[8]) poskytuje základní prostor pro jednotnou právní unifikaci trestných činů, které je možné považovat za kybernetické, napříč jednotlivými zeměmi. Vlastní, mnohdy až velmi strohé vymezení daných trestných činů je věci spíše ku prospěchu, neboť nijak neomezuje vnitrostátní (podrobnější či rozpracovanější) implementaci těchto trestných činů, avšak zároveň zaručuje splnění minimálních požadavků (standardů) všemi ratifikujícími stranami.

I z důvodu značné nejednotnosti v názorech na to, co vše je a co není kybernetická kriminalita, v následující části této kapitoly vymezíme tento pojem, a to jak z hlediska pozitivního, tak negativního.

Nejobecněji je možné kybernetickou kriminalitu definovat **jako jednání namířené proti počítači, případně počítačové síti, nebo jako jednání, při němž je počítač použit jako nástroj pro spáchání trestného činu.** Neopomenutelnou skutečností pro to, aby bylo možné uplatnit definici kyberkriminality, je fakt, že počítačová síť, respektive kyberprostor je pak prostředím, v němž se tato činnost odehrává.

Při definici pojmu kybernetická kriminalita je nutno v prvé řadě **vymezit pojem kriminalita vůbec**. V souvislosti s provozem informačních systémů, výpočetní techniky či komunikačních prostředků dochází k celé řadě jednání, která jsou jistě nežádoucí, ale nejsou postižitelná prostředky trestního práva, přestože mohou být pro společnost značně nebezpečná (škodlivá). Taková jednání *a priori* nemohou být kvalifikována jako počítačová, informační či jakákoliv jiná kriminalita – nejsou totiž kriminalitou vůbec. Při definování pojmu kriminalita (přičemž tuto definici je možno podat z více úhlů pohledu - sociologicky, trestněprávně atd.) se opíráme o definici kriminality jako o **souhrn všech jednání, která lze podřadit pod některou skutkovou podstatu, upravenou trestním zákonem. Podle tohoto vymezení tedy nejsou kriminalitou taková jednání, která nenaplňují žádnou skutkovou podstatu trestného činu, tedy ani přestupku či jiného správního deliktu**. Takové vymezení pojmu kriminalita je poměrně přesné a lze s ním vystačit i v oblasti informační a komunikační techniky.

Pro páchání trestných činů v oblasti ICT však charakteristické, že jsou v rámci jejich spáchání používány takové postupy či prostředky, jejichž užití nenaplňuje žádnou skutkovou podstatu trestného činu, avšak jsou nedílnou součástí či předpokladem pro jednání další, které již postižitelné prostředky trestního práva je.[9] Navíc tyto netrestné postupy či prostředky představují v procesu odhalování a objasňování trestné činnosti důležité komponenty, jejichž identifikace a pochopení hraje významnou roli při odhalování pachatelů tohoto druhu trestné činnosti.[10]

Kybernetická kriminalita, resp. kybernetická trestná činnost, představuje jakousi nejširší množinu pro veškerou trestnou činnost, ke které dochází v prostředí informačních a komunikačních technologií. Delikty páchané v rámci této množiny je možno podle různých hledisek dále třídit a označovat různými pojmy. „Internetová kriminalita", „e-kriminalita", „kyberterorizmus" či např. „pirátství" pak mohou tvořit podmnožiny kybernetické trestné činnosti, přičemž tímto výčtem nedochází k vyčerpání možných podmnožin jednání, které je možné pod pojem kyberkriminalita podřadit.

Pod označením kybernetická trestná činnost bývají v odborných publikacích nejčastěji označena taková kriminální **jednání, při kterých jsou prostředky informačních a komunikačních technologií**:

a) ***užity jako nástroj pro spáchání trestného činu***,

b) ***cílem útoku pachatele***, přičemž tento útok je trestným činem.

Takové vymezení kybernetické kriminality však v dnešní době již neobstojí. Zahrnovalo by totiž i takové trestné činy, při kterých sice dojde k použití informačních technologií, avšak nikoliv v kontextu jejich běžného užívání či určení (např. jde o případy, kdy pachatel ublíží poškozenému na zdraví úderem monitoru či jinou součástí počítače do temene hlavy v úmyslu způsobit ublížení na zdraví; nebo půjde o krádež nákladního automobilu převážejícího počítačové komponenty apod.). Jde o trestné činy, kde je ICT využito mimo svůj rámec určení – např. jako zbraň, jako věc, která má určitou hodnotu vyjádřitelnou penězi, bez ohledu na to, za jakým účelem slouží nebo má sloužit. Při odhalování a objasňování těchto činů se uplatní jiné metodiky vyšetřování (např. metodika vyšetřování krádeží apod.), nikoliv metodika vyšetřování kybernetické kriminality.

Aby bylo možno hovořit o kybernetické kriminalitě, musí být informační a komunikační technologie, které byly ke spáchání trestného činu užity nebo které byly cílem takového činu, zasazeny do určitého kontextu. V tomto duchu je tedy ke dvěma výše uvedeným bodům nutno přiřadit ještě jeden bod, obsahující tuto podmínku. Kybernetická kriminalita pak tedy představuje takovou kriminalitu, kde jsou prostředky informačních a komunikačních technologií:

a) ***užity jako nástroj pro spáchání trestného činu*****,**

b) ***jsou cílem útoku pachatele*****, přičemž tento útok je trestným činem,**

za podmínky, že jsou tyto prostředky užity či zneužity v informačním, systémovém, programovém či komunikačním prostředí (tedy v kyberprostoru)**.**

Takové vymezení kyberkriminality je však stále ještě nedostatečné. Za použití takto stanovených kritérií pro určení, zda je či není konkrétní jednání možno považovat za kybernetickou kriminalitu, dojdeme k závěru, že např. hlediska vymezení účastenství (organizátorství, návod a pomoc) ve smyslu § 24 zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů,[11] je možné spáchat každý úmyslný trestný čin pomocí informačních prostředků (např. osoba přiměje pomocí e-mailových zpráv jiného ke spáchání úmyslného trestného činu vraždy). Obdobně tomu bude i u jiných forem trestné součinnosti (např. podněcování, schvalování trestného činu). Ty lze též spáchat prostřednictvím informačních technologií. **Takováto jednání však za kybernetickou kriminalitu označit nelze**. **Ve svém důsledku by akceptace opačného názoru vedla k jedinému možnému závěru - každý trestný čin, při jehož spáchání pachatel použil jakýmkoliv způsobem informační a komunikační technologie, je kybernetickou kriminalitou**. Z tohoto hlediska by se pak těžko hledaly trestné činy, které za kyberkriminalitu považovat nelze.

Z uvedeného vyplývá, že kybernetickou kriminalitu nepostačí vymezit pouze pozitivně, ale je nutno ji vymezit i výčtem jednání, která zásadně za kybernetickou kriminalitu považovat nelze.

V tomto duchu pak bude možno pod pojem kybernetická kriminalita zařadit trestné činy tří různých kategorií:

1) trestné činy, jejichž individuálním objektem charakterizujícím skutkovou podstatu je přímo ochrana počítačového systému, jeho vybavení a součástí před specifickými druhy útoku resp. oprávněné zájmy osob na nerušené užívání těchto technických prostředků,

2) trestné činy, kde je způsob spáchání prostřednictvím informační a komunikační techniky jedním ze znaků skutkové podstaty,

3) ostatní v úvahu připadající trestné činy, které nespadají do první ani druhé kategorie, avšak které mohou být v konkrétním případě též spáchány prostřednictvím informačních technologií a které odpovídají výše uvedené definici, neboť v rámci jejich odhalování a objasňování se mohou uplatnit obdobné postupy jako při vyšetřování trestných činů z 1. a 2. kategorie (např. obdobně zaměřené znalecké posudky).

[1] SMEJKAL, Vladimír, Tomáš SOKOL a Martin VLČEK. *Počítačové právo.* Praha: C. H. Beck, 1995, s. 99

[2] V současnosti se jedná o celou řadu zařízení, která jsou označována jako počítačový systém.

[3] Blíže např.:

GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Praha: Auditorium, 2008, s. 32 a násl.

Smejkal, Vladimír. Kriminalita v prostředí informačních systémů a rekodifikace trestního zákoníku. Trestněprávní revue, 2003, roč. 2, č. 6, s. 161.

POŽÁR, Josef. Informační bezpečnost. Plzeň: Aleš Čeněk, 2005, s. 249.

[4] MATĚJKA, Michal. *Počítačová kriminalita.* Praha: Computer Press, 2002, s. 5

[5] SMEJKAL, Vladimír. *Kybernetická kriminalita.* Plzeň: Aleš Čeněk, 2015, s. 19

[6] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 2. aktualiz. vyd. Praha: AFCEA, 2015, s. 57 a 73. [online]. [cit.10.7.2016]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/

[7] Dále jen **Úmluva o kyberkriminalitě**. Blíže viz: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[8] Dále jen **Dodatkový protokol**. ETS No. 189 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems

Blíže viz: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189

[9] Např. zasílání nevyžádané pošty (SPAM). Spam někdy může být pouze reklamním (obchodním) sdělením. Takovéto jednání pak není postižitelné prostředky trestního práva. Lze si tak představit například zasílání SPAMu politicky, nábožensky, či jinak motivovaného. Jindy může SPAM obsahovat malware umožňující získat přístupové jméno a heslo k bankovnímu účtu klienta (což je za určitých okolností možné kvalifikovat např. jako přípravu k trestnému činu).

[10] Např. díky komunikaci pachatele s okolím je možno vystopovat IP adresu jeho PC a následně lokalizovat místo připojení pachatele k síti Internet.

[11] Dále jen **trestní zákoník** či **TZK.**

2.2. Klasifikace forem kyberkriminality

Domnívám se, že pokud se chceme zabývat problematikou kyberkriminality, bylo by vhodné alespoň rámcově vymezit, co vše je možné pod tuto trestnou činnost zahrnout. Na závěr této subkapitoly chci proto čtenáři předložit některé klasifikace kybernetické (či počítačové) kriminality tak, jak je vnímají různé právní normy, různí autoři, či organizace, které se věnují boji s kybernetickou kriminalitou. Na těchto členěních chci demonstrovat i genezi pohledu na problematiku kybernetické kriminality.

1. Klasifikace dle Úmluvy o kyberkriminalitě a dle dodatkového protokolu.

Úmluva o kyberkriminalitě dělí kybernetické trestné činy do čtyř kategorií:

1. **trestné činy proti utajování, integritě a dostupnosti počítačových dat a systémů** (*Offences against the confidentiality, integrity and availability of computer data and systems)*,

2. **trestné činy související s počítači** (*Computer-related offences)*,

3. **trestné činy související s obsahem** (*Content-related offences)*,

4. **trestné činy související s porušováním autorských práv a práv souvisejících** (*Offences related to infringements of copyright and related rights)*.

Dodatkový protokol pak definuje další kybernetické trestné činy:

1. **šíření rasistických a xenofobních materiálů pomocí počítačových systémů** (*Dissemination of racist and xenophobic material through computer systems*),

2. **rasisticky a xenofobně motivované vyhrožování** (*Racist and xenophobic motivated threat*),

3. **rasisticky a xenofobně motivované útoky** (*Racist and xenophobic motivated insult*),

4. **popírání, snižování, schvalování nebo ospravedlňování genocidy nebo zločinů proti lidskosti** (*Denial, gross minimisation, approval or justification of genocide or crimes against humanity*).

2. Klasifikace Commitee of Experts on Crime in Cyberspace

Dle Statutu Komise expertů Rady Evropy pro zločin v kyberprostoru (Commitee of Experts on Crime in Cyberspace) z roku 2000 lze kyberzločin rozdělit:

1. **Dle pozice počítače při páchání trestné činnosti:**

- *cíl* (terč) *útoku*;

- *prostředek* (nástroj) *útoku*.

2. **Podle typu činu:**

- *protiprávní jednání tradiční* (např. padělání bankovek aj.)

- *protiprávní jednání nová* (např. phishing, DDoS aj.)[1]

3. Klasifikace dle eEurope+

Tento dokument členil počítačové zločiny na:

1. Zločiny porušující soukromí

- Nelegální sběr, uchovávání, modifikace, zveřejňování a šíření osobních dat.

2. Zločiny se vztahem k obsahu počítače

- Dětská pornografie, rasizmus, vyzývání k násilí aj.

3. Ekonomické

- Neautorizovaný přístup, sabotáž, hackerství, šíření virů, počítačová špionáž, počítačové padělání a podvody.

4. Zločiny se vztahem k duševnímu vlastnictví[2]

4. Klasifikace počítačové trestné činnosti dle kriminalistiky

Porada a Konrád[3] dělí počítačovou kriminalitu do pěti základních skupin.

1. Neoprávněné zásahy do vstupních dat

- Změna vstupního dokladu pro zpracování počítačem,

- vytvoření dokladu obsahujícího nepravdivé údaje pro následné zpracování dat počítačem,

2. **Neoprávněné změny v uložených datech**

- manipulace s daty, neoprávněný zásah do nich a následný návrat k normálu,

3. **Neoprávněné pokyny k počítačovým operacím**

- přímý pokyn k provedení operace, či instalace softwaru provádějícího operace automaticky,

4. **Neoprávněné pronikání do počítačů, počítačového systému a jeho databází**

- informativní vstup do databáze, bez využití informací,
- neoprávněné užívání informací pro vlastní potřeby,
- změny, ničení, či nahrazování informací jinými,
- nelegální „odposlech" a záznam provozu elektronické komunikace,

5. **Napadení cizího počítače, programového vybavení a souborů a dat v databázích**

- vytváření programů sloužících k napadení,
- zavedení viru do programového vybavení počítače,
- vlastní napadení viry, či jinými programy.

5. Zaměření Europolu na některé druhy kyberkriminality dle závažnosti

Europol respektuje Úmluvu o kyberkriminalitě a vychází z členění trestných činů v ní obsažených. Pro podporu boje s kyberkriminalitou a pomoc členským státům došlo, v rámci Europolu, ke vzniku The European Cyber Crime Centre (EC3)[4]. Tento tým jasně deklaroval svoje pole působnosti v rámci boje s kybernetickou trestnou činností a vymezil následující tři oblasti (FP – focal point), kterým se věnuje:

1. **FP TERMINAL – Payment fraud**. Skupina, která se věnuje a poskytuje podporu při řešení online podvodů.

2. **FP Cyborg – High-Tech Crimes**. Skupina, která se věnuje a poskytuje podporu při různých kybernetických útocích, jež ovlivňují kritickou infrastrukturu[5] a informační systémy. Zejména se jedná o útoky typu: Malware, Ransomware, Hacking, Phishing, Identity Theft aj.

3. **FP Twins – Child Sexual Exploitation**. Skupina, která se věnuje a poskytuje podporu při vyšetřování trestné činnosti, při níž dochází k sexuálnímu zneužívání dětí.

6. Klasifikace kyberkriminality dle jejího „vztahu" k digitálnímu prostředí

S rozvojem kyberkriminality jako takové se v posledních letech do popředí stále více dostává názor, dle kterého je možné na kyberkriminalitu pohlížet jako na jednání, které by bylo možné označit termínem „ryzí" či „čistá" kyberkriminalita. Pod takovéto jednání by bylo možné subsumovat pouze takové kybernetické útoky, které se odehrály v kyberprostoru a jejichž cílem a nástrojem byl počítačový systém, případně data. Typicky se pak jedná p útoky mající povahu hackingu, DoS, DDoS útoků, útoků na kritickou infrastrukturu aj.

Ostatní kriminalita páchaná v prostředí kyberprostoru je považována pouze za přenesení „starého" či „běžného" kriminálního jednání do prostředí nového digitálního.

Dle výše uvedeného dělení by pak bylo možné kyberkriminalitu chápat v:

- Užším pojetí („ryzí" kyberkriminalita);
- Širším pojetí („běžné" kriminální jednání v novém prostředí).

Další možné klasifikace kyberkriminality

Existuje i mnoho jiných způsobů klasifikace, pro ilustraci uvádím další možné dělení kyberkriminality.[6]

Na tomto místě si dovolím uvést i klasifikaci, kterou jsem vytvořil na základě vlastních poznatků získaných zejména při interpretaci problematiky kyberkriminality na různých seminářích či konferencích.

Je možné konstatovat, že velmi zjednodušeně lze kyberkriminalitu dělit ze tří hledisek:

1. **Dle četnosti (povahy) útoků:**

a) ***porušování práv autorských*** (viz Internetové (počítačové) pirátství. Jde o jednání, které je v rámci kyberprostoru dominantní a při kterém dochází k porušování intelektuálního vlastnictví. Snaha o potírání tohoto jevu je zjevná zejména za strany soukromých organizací hájících práva autorů.);

b) ***ostatní kybernetické útoky*** (viz projevy kyberkriminality. Vyjma Internetové (počítačové) pirátství.).

2. **Dle postižitelnosti trestním právem:**

a) ***trestním právem řešené jednání*** – některé z uvedených jednání subsumovatelných pod skutkovou podstatu trestného činu;

b) ***trestním právem neřešené (nepostižitelné) jednání*** (některé z uvedených jednání není možné, ani za použití přípustné analogie[7], subsumovat pod zákonné znaky skutkové podstaty trestného činu.).

3. **Dle míry tolerance většinovou společností:**

a) ***společností tolerované jednání*** (nejvíce je tolerováno jednání spočívající v porušování práv autorských);

b) ***společností neakceptované jednání*** (např. dětská pornografie aj.).

---

[1] [online]. [cit.11.3.2010]. Dostupné z: http://assembly.coe.int/documents/WorkingDocs/doc01/edoc9263.htm

Srov. MATĚJKA, Michal. *Počítačová kriminalita.* Praha: Computer Press, 2002, s. 49

[2] Blíže: JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007, s. 92

[3] Blíže: STRAUS, Jiří a kol. *Kriminalistická metodika.* Plzeň: Aleš Čeněk, 2006, s. 272 - 274

[4] *Combating Cybercrime in a Digital Age.* [online]. [cit.7.5.2018]. Dostupné z: https://www.europol.europa.eu/ec3

[5] Pokud jde o vymezení pojmu kritická infrastruktura, pak je v ČR (v případě kyberprostoru) třeba vycházet ze zákona o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Dále jen **zákon o kybernetické bezpečnosti** nebo **ZKB.** Tento zákon v § 2 písm. b) vymezuje pojem kritická informační infrastruktura a prvek nebo systém prvků kritické infrastruktury.

Definice pojmu kritická informační infrastruktura vychází z právních předpisů upravujících oblast krizového řízení. Kritická informační infrastruktura je součástí kritické infrastruktury, která je vymezena zákonem č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) ve znění pozdějších předpisů („dále jen krizový zákon"). Aby mohl být určitý informační systém nebo služba a síť elektronických komunikací zařazena do kritické informační infrastruktury, musí splnit definiční kritéria kritické infrastruktury, jakož i prvku kritické infrastruktury, vymezené krizovým zákonem a dále pak i průřezová a odvětvová kritéria stanovená nařízením vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

V odvětvových kritériích pro určení prvku kritické infrastruktury je od účinnosti zákona a kybernetické bezpečnosti vložen bod VI. *„Komunikační a informační systémy"*, písm G.: *oblast kybernetické bezpečnosti*. Zde jsou stanovena odvětvová kritéria pro určení daného informačního systému, služby nebo sítě elektronických komunikací kritickou informační infrastrukturou.

Nicméně toto vymezení se vztahuje pouze na oblast kybernetické bezpečnosti. Obecně **je možné vymezit kritickou infrastrukturu následovně**:

1. Kritickou infrastrukturou se rozumí prvek kritické infrastruktury nebo systém prvků kritické infrastruktury narušení, jehož funkce by měla závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.

2. Prvkem kritické infrastruktury se rozumí stavba, zařízení, prostředek nebo veřejná infrastruktura určená podle průřezových a odvětvích kritérií, která jsou stanovena nařízením vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

3. Průřezovým kritériem pro určení prvku kritické infrastruktury je hledisko

a) obětí s mezní hodnotou více než 250 mrtvých nebo více než 2 500 osob s následnou hospitalizací po dobu delší než 24 hodin,

b) ekonomického dopadu s mezní hodnotou hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu, nebo

c) dopadu na veřejnost s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125 000 osob.

[6] Srov. PROSISE, Chris a Kevin MANDIVA. *Incident response & komputer forensic, second edition.* Emeryville: McGraw-Hill, 2003, s. 22 a násl.

Dále pak např. *Cybercrime*. [online]. [cit.1.2.2015]. Dostupné z:

http://www.britannica.com/EBchecked/topic/130595/cybercrime/235699/Types-of-cybercrime; aj.

[7] **Analogií se rozumí subsumpce případu v trestním zákoně výslovně neuvedeného, pod zákonné ustanovení podobné, v zákoně uvedené.** Oproti extenzivnímu výkladu je v rámci analogie využíváno ustanovení, které se na subsumovaný případ podle svého smyslu nevztahuje. Extenzivní výklad se realizuje v souladu s účelem trestního zákona a v jeho mezích, kdežto analogie tyto pomyslné hranice překračuje. Užitím analogie dochází k **vyplňování mezer v zákonech**. Jsou jí řešeny případy, které zákonodárce opomněl upravit právní normou. V podmínkách ČR je **nelze využít v neprospěch (k tíži) pachatele** (*in malam partem*).

Blíže viz NOVOTNÝ, František, Josef SOUČEK a kol. *Trestní právo hmotné*. 3. rozš. vyd. Plzeň: Aleš Čeněk, 2010, s. 83

2.3. Kybernetický útok (Cyber attack)

Prosise a Mandiva charakterizují tzv. **„počítačovou bezpečnostní událost"** (kterou lze chápat jako počítačový útok či počítačový trestný čin), jako nezákonnou, nepovolenou, neautorizovanou, nepřijatelnou akci, která zahrnuje počítačový systém či počítačovou síť. Tato akce může být zaměřena například na krádež osobních údajů, spam či jiné obtěžování, zpronevěru, šíření či držení dětské pornografie aj.[1]

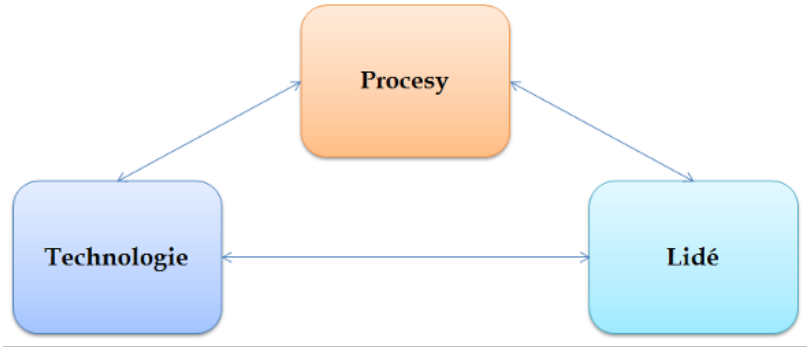
Jirásek a kol. definují kybernetický útok, jako: *„Útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků."*[2]

Takovéto vymezení kybernetického útoku by bylo značně zužující a nepostihující všechny negativní aktivity uživatelů kyberprostoru[3], zejména z toho důvodu, že kumulativně slučuje podmínky poškození IT a získání informací. Kybernetickým útokem přitom může být i jednání v podobě sociálního inženýrství, kde je jediným cílem získat informace, či naopak útok DoS, či DDoS, kde může být jediným cílem potlačení (tedy nikoliv poškození) funkčnosti jednoho či více počítačových systémů, případně poskytovaných služeb.

Na základě výše uvedeného je tedy možné **kybernetický útok**[4] definovat jako **jakékoli protiprávní jednání útočníka v kyberprostoru, které směřuje proti zájmům jiné osoby**. Tato jednání nemusí mít vždy podobu trestného činu, podstatné je, že narušují běžný způsob života poškozeného. Kybernetický útok může být dokonán, stejně jako může být ve stádiu přípravy či pokusu.[5]

Kybernetický trestný čin musí být zároveň kybernetickým útokem, avšak ne každý kybernetický útok musí být trestným činem. Řadu kybernetických útoků je, i díky absenci trestněprávní normy, možné subsumovat pod jednání, které bude mít povahu správněprávního, či občanskoprávního deliktu, případně se nemusí jednat o jednání, které je postižitelné jakoukoli právní normou (může jít např. pouze o nemorální či nechtěné jednání).

Úspěšnost kybernetického útoku typicky spočívá v porušení některého z prvků, které tvoří kybernetickou bezpečnost (**lidé, procesy a technologie**). **Tyto prvky je třeba uplatňovat, případně modifikovat v průběhu celého jejich životního cyklu. Zejména jde o prevenci, detekci a rekci na útok.**[6] Bezpečnost IT, informací a dat je také přímo závislá na repektování principů „C" „I" „A".



Obrázek 8 - Prvky kybernetické bezpečnosti

Pokud chceme definovat pojem kybernetický útok, je vhodné využít i definice, které vyplývají ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).[7] Tento zákon totiž definuje v § 7 pojmy kybernetická bezpečnostní událost a kybernetický bezpečnostní incident. **Kybernetickou bezpečnostní událostí** je *„událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací."* De facto jde o událost bez zatím reálného negativního následku pro daný komunikační nebo informační systém, ve své podstatě se jedná pouze o hrozbu, která však musí být reálná.

Kybernetickým bezpečnostním incidentem je *„narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události."* Kybernetický bezpečnostní incident tak představuje samotné narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací, tj. narušení informačního nebo komunikačního systému s negativním dopadem.

---

[1] PROSISE, Chris a Kevin MANDIVA. *Incident response & komputer forensic, second edition.* Emeryville : McGraw-Hill, 2003, s. 13

Srov. dále CASEY, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Second Edition.* London: Academic Press, 2004, s. 9 a násl.

[2] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 2. aktualiz. vyd. Praha: AFCEA, 2015, s. 59. Dostupný online: http://afcea.cz/cesky-slovnik-pojmu-kyberneticke-bezpecnosti/

[3] V uvedené definici chybí zejména vymezení jakékoliv jiné motivace útočníka, než té, která spočívá ve *...způsobení poškození či zisku strategicky důležitých informací.* Jako příklad, který tato definice nepostihuje, lze uvést ekonomicky motivované útoky, jejichž počet v současnosti dramaticky roste.

[4] Od pojmu kybernetický útok je třeba odlišit pojem **bezpečnostní incident**, který představuje narušení bezpečnosti IS/IT a pravidel definovaných k jeho ochraně (bezpečnostní politika).

[5] Např. útok virem Conficker, který vytvořil Botnet. Tím byl útok dokonán. Otázkou však zůstává, k jakým účelům bude tato síť případně využita (může se jednat o přípravu daleko vážnějšího kybernetického útoku).

[6] Blíže viz SVOBODA, Ivan. *Řešení kybernetické bezpečnosti.* Přednáška v rámci CRIF Academy. (23. 9. 2014)

[7] Dále jen **zákon o kybernetické bezpečnosti či ZKB**.

2.4. SHRNUTÍ/ HLAVNÍ VÝSTUPY Z KAPITOLY

SHRNUTÍ/ HLAVNÍ VÝSTUPY Z KAPITOLY

- Pro pochopení problematiky kybernetických útoků a kybernetické kriminality je třeba znát základní terminologii, která se zvolenou oblastí bezprostředně souvisí. Tato kapitola prezentuje vybrané technické, ale i legální pojmy.
- Nelze nalézt oblast lidské činnosti, kde by se přímo nebo zprostředkovaně nevyužívala výpočetní technika, resp. informační systém nebo informační či komunikační technologie.
- Pojem kyberkriminalita má obdobný charakter jako pojmy „násilná kriminalita“, „kriminalita mladistvých“, „ekonomická kriminalita“ apod. Takovýmito názvy jsou označovány skupiny trestných činů mající určitý společný faktor, jako např. způsob provedení, osobu pachatele (alespoň druhově) apod. Ve své podstatě přitom může jít o velmi různorodou směsici trestných činů, spojených oním společným faktorem (počítačem, programem, daty).
- Kybernetickou kriminalitu lze definovat jako jednání namířené proti počítači, případně počítačové síti, nebo jako jednání, při němž je počítač použit jako nástroj pro spáchání trestného činu. Neopomenutelnou skutečností pro to, aby bylo možné uplatnit definici kyberkriminality, je fakt, že počítačová síť, respektive kyberprostor je pak prostředím, v němž se tato činnost odehrává.
- Kybernetická trestná činnost představuje takové kriminální jednání, při kterých jsou prostředky informačních a komunikačních technologií:
  - užity jako nástroj pro spáchání trestného činu,
  - cílem útoku pachatele, přičemž tento útok je trestným činem.
  - za podmínky, že jsou tyto prostředky užity či zneužity v informačním, systémovém, programovém či komunikačním prostředí (tedy v kyberprostoru).
- Kybernetickou kriminalitu nepostačí vymezit pouze pozitivně, ale je nutno ji vymezit i výčtem jednání, která zásadně za kybernetickou kriminalitu považovat nelze.
- Kybernetický útok lze definovat jako jakékoli protiprávní jednání útočníka v kyberprostoru, které směřuje proti zájmům jiné osoby.
- Kybernetickou bezpečnostní událostí je *„událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.“*
- Počítačovými daty rozumí *„jakékoli vyjádření faktů, informací nebo pojmů ve formě vhodné pro zpracování v počítačovém systému, včetně programu způsobilého zapříčinit provedení funkce počítačovým systémem.“*
- Informace *„jsou údaje, které byly zpracovány do podoby užitečné pro příjemce. Každá informace je tedy údajem, datem, ale jakákoli uložená data se nemusejí nutně stát informací.“*

KLÍČOVÁ SLOVA K ZAPAMATOVÁNÍ

- kyberkriminalita
- kybernetický útok
- kybernetická bezpečnostní událost
- trestná činnost
- kyberprostor

KONTROLNÍ OTÁZKY

- Co to je kybernetická kriminalita?
- Co není kybernetickou kriminalitou?
- Co je to kybernetický útok?
- Jaký je rozdíl mezi kybernetickou kriminalitou a kybernetickým útokem?
- Jaký je rozdíl mezi daty a informacemi?
- Co představuje triáda CIA?

3. Trestněprávní ochrana před kyberkriminalitou

Snahy o právní regulaci a postih trestné činnosti páchané prostředky informačních a komunikačních technologií je možné vypozorovat de facto již od počátku těchto negativních aktivit. Kybernetická trestná činnost je značně odlišná od jiných druhů kriminality, přičemž tato odlišnost spočívá především v možnosti jejího dynamického vývoje a okamžité změny (dle úspěšnosti či neúspěšnosti toho kterého typu útoku), což ve vztahu k legislativě může přinášet určité problémy.

V trestním právu hmotném platí zásada, že není možné využít analogie k tíži pachatele (*in malam partem)*. Přesto je možné kybernetické útoky mnohdy subsumovat pod zákonné ustanovení určité skutkové podstaty, byť tato skutková podstata původně směřovala na „tradičnější způsoby" spáchání trestného činu (typicky se jedná například o útoky spojené s porušováním práv autorských, zneužívání dětí k výrobě pornografie aj.). Avšak existuje celá řada útoků nových, u nichž tato možnost v úvahu nepřichází. V takových případech se legislativci jednotlivých zemí zatím především snaží *ad hoc* reagovat na tyto nové druhy trestné činnosti a vyplňují tak slepá místa ve vnitrostátní právní úpravě.

Před vlastní analýzou stávající platné a účinné legislativy v oblasti kyberkriminality je třeba podotknout, že nejen v rámci Evropské unie je zřetelná snaha po implementaci účinnějších právních nástrojů, které by byly schopné včas a adekvátně reagovat na kyberkriminalitu. Dochází tak k postupnému odstraňování rozporů a nedostatků v právních normách členských států EU a dalších států, které se rozhodly aktivně zapojit do boje s kybernetickou trestnou činností.

Jedním z prvních dokumentů věnujících se problematice kyberkriminality, přijatých na mezinárodní úrovni, je **Manuál OSN o prevenci a kontrole trestných činů spojených s počítači** (Havana, 1990).[1]

„Způsoby ochrany dat a informačních systémů jsou dnes předmětem nejednoho vědního výzkumu, ovšem toliko technická ochrana těchto systémů a dat bez právního podkladu může být neefektivní v důsledku nejasného vymezení, kam až je možno při takové ochraně zajít. V tomto kontextu se naplno projevuje nesoulad právních úprav jednotlivých států s právními úpravami států ostatních. Díky rozvoji počítačových a informačních technologií, které udávají mezinárodní charakter kybernetických trestných činů, je efektivní ochrana počítačových systémů a dat nemyslitelná bez existence mezinárodního resp. nadnárodního právního rámce, a to nejen mezi členskými státy EU, ale v celosvětovém měřítku."

---

[1] *United Nations Manual on the prevention and control of computer-related crime.* [online]. [cit.20.8.2016]. Dostupné z: http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf

3.1. Kybernetická trestná činnost v mezinárodních dokumentech a v dokumentech ES/EU

Na prvním místě je třeba zmínit Úmluvu o kyberkriminalitě a dodatkový protokol k ní, neboť se jedná o dva nejvýznamnější právní dokumenty, které přispívají k ochraně společnosti před kyberkriminalitou tím, že stanoví základní rámec trestných kybernetických činů a zároveň stanoví prostředky pro odhalování a vyšetřování této kriminality. Dále budou uvedeny právní dokumenty EU a ES, které souvisí s problematikou kyberkriminality.

3.1.1 Úmluva Rady Evropy č. 185 o kyberkriminalitě

Úmluva o kyberkriminalitě představuje nejvýznamnější právní dokument týkající se kyberkriminality a jejím hlavním účelem je sjednotit národní právní úpravu v oblasti kyberkriminality. Výše uvedené se realizuje tím, že Úmluva o kyberkriminalitě stanoví smluvním stranám povinnost implementovat do národních právních řádů takové nástroje, které umožní postih definovaných kybernetických trestných činů. Právě důkladná definice skutkové podstaty trestného činu je podmínkou k tomu, aby bylo možné užít norem trestního práva v kyberprostoru. Dále Úmluva o kyberkriminalitě vytváří právní rámec pro jednotný a společný postup proti pachatelům těchto trestných činů bez ohledu na místo spáchání trestného činu.

Úmluvu o kyberkriminalitě schválil Výbor ministrů Rady Evropy na svém 109. zasedání dne 8. listopadu 2001. Úmluva o kyberkriminalitě byla otevřena k podpisu 23. listopadu 2001 v Budapešti.[1] V platnost vstoupila tato úmluva dne 1. července 2004.

Česká republika podepsala Úmluvu o kyberkriminalitě dne 9. února 2005 a ratifikovala ji 22. srpna 2013 s tím, že tato úmluva vstoupila v platnost 1. prosince 2013. Členské státy EU se zavázaly ratifikovat Úmluvu o kyberkriminalitě a včlenit do svých právních řádů taková ustanovení, která by umožňovala objasňovat a vyšetřovat uvedenou trestnou činnost.[2] Úmluva o kyberkriminalitě byla rovněž podepsána a ratifikována například Spojenými státy americkými, Japonskem aj.

Úmluva o kyberkriminalitě[3] se skládá z **preambule** a **48 článků**, které jsou rozděleny do 4 kapitol:

1. **Používané pojmy** (*Use of terms*)
2. **Opatření, která mají být přijata na vnitrostátní úrovni** (*Measures to be taken at the national level*)

   Část 1 – Trestní právo hmotné (*Substantive criminal law.* Čl. 2 -13)

   Část 2 – Procesní právo (*Procedural law.* Čl. 14 - 21)

   Část 3 – Soudní pravomoc (*Judrisdiction.* Čl. 22)
3. **Mezinárodní spolupráce** (*International Co-operation*)

   Část 1 – Obecné zásady (*General principles.* Čl. 23 – 28)

   Část 2 – Zvláštní ustanovení (*Specific provisions.* Čl. 29 – 35)
4. **Závěrečná ustanovení** (*Final provisions*)

Významným krokem ke sjednocení práva je definování čtyř základních skupin trestných činů (viz kap. II; čl. 2 – 13) a zakotvení dalších obecných institutů z trestního práva hmotného. Právě jednotné definování (pojmenování) kybernetických útoků umožní jejich efektivnější stíhání v zemích, které Úmluvu o kyberkriminalitě ratifikovaly. Konkrétně se jedná o:

1) **trestné činy proti utajování, integritě a dostupnosti počítačových dat a systémů** (*Offences against the confidentiality, integrity and availability of computer data and systems.* Čl. 2-6),

2) **trestné činy související s počítači** (*Computer-related offences.* Čl. 7-8),

3) **trestné činy související s obsahem** (*Content-related offences*. Čl. 9),

4) **trestné činy související s porušováním autorských práv a práv souvisejících** (*Offences related to infringements of copyright and related rights.* Čl. 10).

Z hlediska obecných hmotněprávních principů je dále definována trestněprávní odpovědnost za pokus a účastenství (*Attempt and aiding or abetting.* Čl. 11)[4] a trestněprávní odpovědnost právnické osoby (*Corporate liability*)[5] za trestný čin podle Úmluvy o kyberkriminalitě.

3.1.2 Dodatkový protokol Rady Evropy č. 189 k Úmluvě o kyberkriminalitě

Dodatkový protokol Rady Evropy č. 189 k Úmluvě o kyberkriminalitě[6], který byl přijat 28. ledna 2003[7], definuje okruh trestných činů, jimž se Úmluva o kyberkriminalitě nevěnuje. V Úmluvě o kyberkriminalitě chybí trestné činy, které spočívají v šíření určitého *„závadného materiálu“*.[8] Dodatkový protokol vymezuje trestné činy, jež spočívají především v šíření materiálů s obsahem rasistickým, xenofobním, či jinak projevujícím rasovou nesnášenlivost. Důvodem nezařazení předmětných trestných činů do Úmluvy o kyberkriminalitě bylo zejména podepsání a následné přijetí Úmluvy o kyberkriminalitě ze strany USA.[9]

Dodatkový protokol se skládá z **preambule** a **16 článků**, které jsou rozděleny do 4 kapitol:

1. **Obecná ustanovení** (*Common provisions*)

2. **Opatření, která mají být přijata na vnitrostátní úrovni** (*Measures to be taken at the national level*)

   - Článek 3 – Šíření rasistického a xenofobního materiálu skrze počítačový systém (*Dissemination of racist and xenophobic material through computer systems*)

   - Článek 4 – Rasisticky a xenofobně motivovaná výhrůžka (*Racist and xenophobic motivated threat*)

   - Článek 5 – Rasisticky a xenofobně motivovaná urážka (*Racist and xenophobic motivated insult*)

   - Článek 6 – Popírání, hrubé zlehčování, schvalování nebo ospravedlňování genocidy nebo zločinů proti lidskosti (*Denial, gross minimisation, approval or justification of genocide or crimes against humanity*)

3. **Vztah mezi Úmluvou o kyberkriminalitě a Dodatkovým protokolem** *(Relations between the Convention and this Protocol)*

4. **Závěrečná ustanovení** (*Final provisions*)

V **kapitole první** je upraven účel Dodatkového protokolu a je zde vymezen pojem – rasistický a xenofobní materiál. Dle čl. 1 odst. 1 Dodatkového protokolu se rasistickým a xenofobním materiálem 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.“*

3.1.3 Dokumenty EU/ES sloužící k harmonizaci právních úprav při potírání kybernetické trestné činnosti

Zejména díky specifičnosti spočívající v neohraničenosti kyberkriminality a potřebě efektivní mezinárodní spolupráce se EU snaží sblížit právní úpravu jednotlivých členských států tak, aby bylo možné tento negativní jev účinněji postihovat. Prostředkem pro sbližování práva jednotlivých zemí EU jsou především rámcová rozhodnutí, směrnice, a další dokumenty EU/ES. Z pohledu boje s kyberkriminalitou jsou nejvýznamnějšími následující dokumenty:

- *Směrnice Rady 91/250/EHS* o právní ochraně počítačových programů
- *Rozhodnutí Rady 92/242/EHS* o bezpečnosti informačních systémů
- *Směrnice Evropského parlamentu a Rady č. 98/34/ES* o postupu při poskytování informací v oblasti norem a technických předpisů ve znění směrnice *č. 98/48/ES*
- *Směrnice č. 2000/31/ES* o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu („směrnice o elektronickém obchodu“)
- *Rámcové rozhodnutí Rady 2000/375/JHA* o boji proti dětské pornografii na internetu
- *Rámcové rozhodnutí Rady 2001/413/SVV* o potírání podvodů a padělání bezhotovostních platebních prostředků
- *Směrnice Evropského parlamentu a Rady č. 2002/21/EC* o společném regulačním rámci pro sítě a služby elektronických komunikací (rámcová směrnice)
- *Směrnice Evropského parlamentu a Rady č. 2002/19/EC* o přístupu k sítím elektronických komunikací a přidruženým zařízením a o jejich propojení (přístupová směrnice)
- *Směrnice Evropského parlamentu a Rady č. 2002/20/EC* o oprávnění pro sítě a služby elektronických komunikací (autorizační směrnice)
- *Směrnice Evropského parlamentu a Rady č. 2002/22/EC* o universální službě a uživatelských právech týkajících se sítí a služeb elektronických komunikací (směrnice o universální službě)
- *Směrnice Evropského parlamentu a Rady 2002/58/EC* týkající se zpracovávání osobních údajů a ochrany soukromí v oblasti elektronických komunikací (směrnice o ochraně údajů v elektronických komunikacích)
- *Směrnice Komise č. 2002/77/ES* o hospodářské soutěži na trzích s elektronickými komunikačními sítěmi a službami (soutěžní směrnice)
- *Rámcové rozhodnutí Rady EU č. 2002/584/JHA* o evropském zatýkacím rozkazu a postupech předávání mezi členskými státy
- *Rámcové rozhodnutí Rady 2004/68/SVV* o boji proti pohlavnímu vykořisťování dětí a dětské pornografii
- ***Rámcové rozhodnutí Rady 2005/222/SVV* o útocích proti informačním systémům**
- *Sdělení Komise Evropskému parlamentu, Radě, Hospodářskému a sociálnímu výboru a Výboru regionů* - Boj proti spamu a špionážnímu („spyware“) a škodlivému softwaru („malicious software“) *ze dne 15. 11. 2006*
- *Sdělení Komise Evropskému Parlamentu, Radě a Evropskému výboru regionů* k obecné politice v boji proti počítačové kriminalitě *ze dne 22. 5. 2007*
- *Závěry Rady* o společné pracovní strategii a konkrétních opatřeních v oblasti boje proti počítačové trestné činnosti *ze dne 27. 11. 2008*
- *Sdělení Komise Evropskému Parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a výboru regionů* o ochraně kritické informační infrastruktury „Ochrana Evropy před rozsáhlými počítačovými útoky a narušením: zvyšujeme připravenost, bezpečnost a odolnost“ *ze dne 30. 3. 2009*
- *Sdělení komise Radě a Evropskému parlamentu*, Řešení trestné činnosti v digitálním věku: zřízení Evropského centra pro boj proti kyberkriminalitě. 2012
- *Nařízení Evropského parlamentu a Rady (EU) č. 526/2013*, o Agentuře Evropské unie pro bezpečnost sítí a informací (ENISA) a o zrušení nařízení (ES) č. 460/2004, ze dne 21. května 2013
- *Směrnice Evropského parlamentu a Rady 2013/40/EU*, o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV, ze dne 12. srpna 2013
- *Nařízení Evropského parlamentu a Rady (EU) č. 513/2014*, kterým se jako součást Fondu pro vnitřní bezpečnost zřizuje nástroj pro finanční podporu policejní spolupráce, předcházení trestné činnosti, boje proti trestné činnosti a řešení krizí a zrušuje rozhodnutí Rady 2007/125/SVV, ze dne 16. dubna 2014
- *Nařízení Evropského parlamentu a Rady (EU) č. 910/2014*, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, ze dne 23. července 2014 (eIDAS, resp. Nařízení eIDAS)
- *Nařízení Evropského parlamentu a Rady (EU) 2016/794*, o Agentuře Evropské unie pro spolupráci v oblasti prosazování práva (Europol) a o zrušení a nahrazení rozhodnutí 2009/371/SVV, 2009/934/SVV, 2009/935/SVV, 2009/936/SVV a 2009/968/SVV, ze dne 11. května 2016
- *Nařízení Evropského parlamentu a Rady (EU) 2016/679* ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
- *Směrnice Evropského parlamentu a Rady (EU) 2016/1148*, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů

v Unii, ze dne 6. července 2016 (NIS Directive)[10]
- *Závěry Rady o společné pracovní strategii a konkrétních opatřeních v oblasti boje proti počítačové trestné činnosti* ze dne 27. listopadu 2008
- *Sdělení Komise Evropskému Parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a výboru regionů o ochraně kritické informační infrastruktury „Ochrana Evropy před rozsáhlými počítačovými útoky a narušením: zvyšujeme připravenost, bezpečnost a odolnost"* ze dne 30. 3. 2009[11]

3.1.4 Právní normy České republiky

V souvislosti s kybernetickou trestnou činností a kybernetickou bezpečností je třeba uvést i právní normy ČR, které mají bezprostřední vztah k této problematice:

- Zákon č. 40/2009 Sb., trestní zákoník
- Zákon č. 141/1961 Sb., o trestním řízení soudním
- Zákon č. 218/2003 Sb., zákon o soudnictví ve věcech mládeže
- Zákon č. 121/2000 Sb., autorský zákon
- Zákon č. 127/2005 Sb., o elektronických komunikacích
- Zákon č. 480/2004 Sb., o některých službách informační společnosti
- Zákon č. 273/2008 Sb., o Policii České republiky
- Zákon č. 89/2012 Sb., občanský zákoník
- Zákon č. 110/2019 Sb., o zpracování osobních údajů
- Zákon č. 14/1993 Sb., o opatřeních na ochranu průmyslového vlastnictví
- Zákon č. 441/2003 Sb., o ochranných známkách
- Zákon č. 527/1990 Sb., o vynálezech, průmyslových vzorech a zlepšovacích návrzích
- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů
- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce
- Zákon č. 160/1999 Sb., o svobodném přístupu k informacím
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

3.1.5 Právní normy Polska

- FIX ME

3.1.6 Právní normy Portugalska

- FIX ME

---

[1] Seznam států, které podepsaly a ratifikovaly Úmluvu o kyberkriminalitě, je možné nalézt na:

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=F6wSLE5D.

[2] Tento závazek je dán v čl. 14 - 21 Úmluvy o kyberkriminalitě.

[3] Kompletní znění Úmluvy je možné nalézt na: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[4] Tento požadavek je v českém trestním právu zcela realizován instituty *pokus trestného činu* (§ 21 a 111 TZK) a *účastenství* (§ 24 a 111 TZK).

[5] Trestněprávní odpovědnost právnických osob je v českém právním prostředí realizována na základě zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, ve znění pozdějších předpisů.

[6] *ETS No. 189 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.* [online]. [cit.20.8.2016]. Dostupné z: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008160f

[7] Seznam států, které podepsaly a ratifikovaly Dodatkový protokol, je možné nalézt na:

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=F6wSLE5D

[8] Vyjma dětské pornografie, která je přímo obsažena v čl. 9 Úmluvy o kyberkriminalitě.

[9] Právě problematika rasismu a xenofobie je v USA tématem nacházejícím se v „šedé zóně", neboť některá prohlášení lze považovat za trestný čin a jiná naopak ne. Např. Ne všechny projevy rasismu jsou v **USA** považovány za trestný čin, viz **První dodatek Ústavy USA** – *Kongres nevydá žádný zákon, který by nerespektoval svobodu vyznání, nebo by obsahoval zákaz volného výkonu (bohoslužebných úkonů), nebo oklešťující svobodu slova nebo tisku nebo právo lidu pokojně se shromažďovat a podávat petici vládě s cílem nápravy křivd***. Aby se jednalo o protiprávní jednání či trestný čin, je třeba prokázat reálnost hrozby, v opačném případě by se jednalo o narušení prvního dodatku.** Oproti tomu jsou projevy rasismu ve **Francii** či **SRN**, stejně jako v **ČR** považovány za trestný čin.

[10] K některým uvedeným dokumentům blíže viz: VOLEVECKÝ, Petr. Kybernetická trestná činnost v mezinárodních dokumentech a v dokumentech ES/EU. In *Trestní právo,* 2009, roč. 12, č. 7-8, s. 26-39. Veškeré předpisy práva EU jsou dostupné i v české verzi na *EUR-lex.* [online]. [cit.20.8.2016]. Dostupné z: http://eur-lex.europa.eu/homepage.html

[11] KOLOUCH, Jan a Petr VOLEVECKÝ. *Trestněprávní ochrana před kybernetickou kriminalitou.* Praha: Policejní akademie České republiky v Praze, 2013, s. 76

3.2. Hmotněprávní aspekty kybernetické trestné činnosti v ČR

3.2.1 Kybernetické trestné činy ve zvláštní části trestního zákoníku

Z hlediska kybernetické trestné činnosti obsahuje trestní zákoník speciální skutkové podstaty trestných činů, které jsou zaměřeny na kyberkriminalitu, respektive některé kybernetické útoky.

Kybernetické trestné činy jsou v nejobecnější rovině z hlediska využití informačních a komunikačních technologií tříděny na trestné činy, při kterých jsou tyto prvky užity jako nástroj umožňující spáchání trestného činu, přičemž skutková podstata trestného činu obsahuje použití těchto prostředků jako znak skutkové podstaty, a na trestné činy, při kterých jsou prvky informačních a komunikačních technologií terčem útoku pachatele, tedy představují individuální objekt resp. hmotný předmět útoku.

Zákonodárce zařadil do zvláštní části trestního zákoníku řadu skutkových podstat trestných činů, které buď obsahují znaky mající vztah k informačním a komunikačním technologiím, nebo mohou být naplněny kybernetickým útokem. Mezi tyto činy je možné zařadit:

- § 180 neoprávněné nakládání s osobními údaji
- § 181 poškození cizích práv
- § 182 porušení tajemství dopravovaných zpráv
- § 183 porušení tajemství listin a jiných dokumentů uchovávaných v soukromí
- § 184 pomluva
- § 191 šíření pornografie
- § 192 výroba a jiné nakládání s dětskou pornografií
- § 193 zneužití dítěte k výrobě pornografie
- § 193b navazování nedovolených kontaktů s dítětem
- § 205 krádež
- § 206 neoprávněné užívání cizí věci
- § 209 podvod
- § 213 provozování nepoctivých her a sázek
- § 214 podílnictví
- § 216 legalizace výnosů z trestné činnosti
- § 228 poškození cizí věci
- § 230 neoprávněný přístup k počítačovému systému a nosiči informací
- § 231 opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat
- § 232 poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti
- § 234 neoprávněné opatření, padělání a pozměnění platebního prostředku
- § 236 výroba a držení padělatelského náčiní
- § 264 zkreslení údajů a nevedení podkladů ohledně vývozu zboží a technologií dvojího užití
- § 268 porušení práv k ochranné známce a jiným označením
- § 267 zkreslení údajů a nevedení podkladů ohledně zahraničního obchodu s vojenským materiálem
- § 269 porušení chráněných průmyslových práv
- § 270 porušení autorského práva, práv souvisejících s právem autorským a práv k databázi
- § 272 obecné ohrožení
- § 276 poškození a ohrožení provozu obecně prospěšného zařízení
- § 287 šíření toxikomanie
- § 290 získání kontroly nad vzdušným dopravním prostředkem, civilním plavidlem a pevnou plošinou
- § 291 ohrožení bezpečnosti vzdušného dopravního prostředku a civilního plavidla

- § 311 teroristický útok
- § 316 vyzvědačství
- § 317 ohrožení utajované informace
- § 345 křivé obvinění
- § 348 padělání a pozměnění veřejné listiny
- § 353 nebezpečné vyhrožování
- § 354 nebezpečné pronásledování
- § 355 hanobení národa, rasy, etnické nebo jiné skupiny osob
- § 356 podněcování k nenávisti vůči skupině osob nebo k omezování práv a svobod
- § 357 šíření poplašné zprávy
- § 361 účast na organizované zločinecké skupině
- § 364 podněcování k trestnému činu
- § 365 schvalování trestného činu
- § 400 genocidum
- § 403 založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka
- § 404 projev sympatií k hnutí směřujícímu k potlačení práv a svobod člověka
- § 405 popírání, zpochybňování, schvalování a ospravedlňování genocidia
- § 407 podněcování útočné války

Tyto kybernetické trestné činy podle trestního zákoníku je možné třídit podle mnoha různých kritérií. Mezi nejčastěji používané třídění kybernetických trestných činů patří již výše zmíněné třídění na:[1]

a) **trestné činy, při jejichž páchání představují prostředky informačních a komunikačních technologií předmět ochrany** (tedy jsou terčem kybernetického útoku):

- § 182 porušení tajemství dopravovaných zpráv
- § 183 porušení tajemství listin a jiných dokumentů uchovávaných v soukromí
- § 206 neoprávněné užívání cizí věci
- § 228 poškození cizí věci
- § 230 neoprávněný přístup k počítačovému systému a nosiči informací
- § 232 poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti
- § 234 neoprávněné opatření, padělání a pozměnění platebního prostředku
- § 264 zkreslení údajů a nevedení podkladů ohledně vývozu zboží a technologií dvojího užití
- § 267 zkreslení údajů a nevedení podkladů ohledně zahraničního obchodu s vojenským materiálem
- § 270 porušení autorského práva, práv souvisejících s právem autorským a práv k databázi
- § 290 získání kontroly nad vzdušným dopravním prostředkem, civilním plavidlem a pevnou plošinou
- § 291 ohrožení bezpečnosti vzdušného dopravního prostředku a civilního plavidla
- § 311 teroristický útok
- § 317 ohrožení utajované informace

b) **trestné činy, při jejichž páchání jsou prostředky informačních a komunikačních technologií užity ke spáchání trestného činu**:

- § 180 neoprávněné nakládání s osobními údaji
- § 181 poškození cizích práv
- § 182 porušení tajemství dopravovaných zpráv
- § 184 pomluva

- § 191 šíření pornografie
- § 192 výroba a jiné nakládání s dětskou pornografií
- § 193 zneužití dítěte k výrobě pornografie
- § 193b navazování nedovolených kontaktů s dítětem
- § 205 krádež
- § 209 podvod
- § 213 provozování nepoctivých her a sázek
- § 214 podílnictví
- § 216 legalizace výnosů z trestné činnosti
- § 230 neoprávněný přístup k počítačovému systému a nosiči informací
- § 231 opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat
- § 234 neoprávněné opatření, padělání a pozměnění platebního prostředku
- § 236 výroba a držení padělatelského náčiní
- § 268 porušení práv k ochranné známce a jiným označením
- § 269 porušení chráněných průmyslových práv
- § 272 obecné ohrožení
- § 276 poškození a ohrožení provozu obecně prospěšného zařízení
- § 287 šíření toxikomanie
- § 316 vyzvědačství
- § 345 křivé obvinění
- § 348 padělání a pozměnění veřejné listiny
- § 353 nebezpečné vyhrožování
- § 354 nebezpečné pronásledování
- § 355 hanobení národa, rasy, etnické nebo jiné skupiny osob
- § 356 podněcování k nenávisti vůči skupině osob nebo k omezování práv a svobod
- § 357 šíření poplašné zprávy
- § 361 účast na organizované zločinecké skupině
- § 364 podněcování k trestnému činu
- § 365 schvalování trestného činu
- § 400 genocidum
- § 403 založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka
- § 407 podněcování útočné války

Vedle uvedených ustanovení zvláštní části trestního zákoníku se k problematice kybernetických trestných činů vztahuje též § 120 TZK, které stanovuje, že „*uvést někoho v omyl či využít něčího omylu lze i provedením zásahu **do počítačových informací nebo** dat, zásahu do **programového vybavení počítače** nebo provedením **jiné operace na počítači**, zásahu do **elektronického nebo jiného technického zařízení**, včetně zásahu do **předmětů sloužících k ovládání takového zařízení**, anebo využitím takové operace či takového zásahu provedeného jiným*."

[1] Některé trestné činy je vzhledem k dikci jejich skutkových podstat možné zařadit do obou kategorií (tato ustanovení chrání prostředky informačních a komunikačních technologií, ale zároveň obsahují znaky zneužití těchto technologií).

3.3. Hmotněprávní aspekty kybernetické trestné činnosti v Polsku

Zákonodárce zařadil do trestního zákoníku řadu trestných činů, které buď obsahují prvky související s informačními a komunikačními technologiemi, nebo mohou být naplněny kybernetickým útokem. Tyto trestné činy mohou zahrnovat:

Článek 126a. Veřejné podněcování ke spáchání trestného činu

Článek 130. špionáž

Článek 132. Zpravodajské dezinformace

Článek 133. Urážka národa nebo Polské republiky

Článek 135. Útok na prezidenta Polské republiky nebo jeho urážka

Článek 136. Aktivní útok nebo urážka představitele cizího státu

Článek 137. Veřejná urážka státního znaku nebo symbolu

Článek 151. Úmysl spáchat sebevraždu a poskytnutí pomoci

Článek 165 Způsobení veřejného ohrožení

Článek 190. Trestní hrozba

Článek 190a. Stalking

Článek 191. Vynucení určitého jednání, zanechání nebo potlačení

Článek 191a. Záznam obrazu nahé osoby

Článek 196. Urážka náboženského cítění jiných osob

Článek 200a. Elektronický kontakt s nezletilou osobou pro pedofilní účely

Článek 200b. Veřejná propagace pedofilního obsahu

Článek 202. Prezentace a šíření pornografie

Článek 212. Pomluva

Článek 216. Hanobení osoby

Článek 224a. Falešné hlášení o hrozbě

Článek 226. Urážka veřejného činitele nebo ústavního orgánu Polské republiky

Článek 227. Zpronevěra funkce veřejného činitele

Článek 228. Podplácení veřejného činitele

Článek 229. Úplatkářství

Článek 230. Pasivní placená záštita

Článek 230a. Aktivní placený patronát

Článek 232. ovlivňování činnosti soudu

Článek 234. Křivé obvinění

Článek 235. vytváření falešných důkazů

Článek 236. Zadržování důkazů o nevině podezřelého

Článek 238. Nepravdivé oznámení trestného činu

Článek 239 Podporování a navádění

Článek 240. Trestný čin neoznámení trestného činu

Článek 241. Nezákonné šíření zpráv z přípravného řízení nebo soudního procesu

Článek 244. Nesplnění trestních opatření nařízených soudem

Článek 245 Použití násilí nebo výhrůžek s cílem ovlivnit účastníka řízení

Článek 246. Vydírání veřejného činitele, aby poskytl svědectví, vysvětlení, informace nebo prohlášení

Článek 250. nezákonné ovlivňování osoby oprávněné volit

Článek 251 Porušení tajnosti hlasování

Článek 255 Veřejné podněcování ke spáchání přestupku nebo daňového trestného činu nebo jejich vychvalování

Článek 255a. Šíření obsahu usnadňujícího spáchání teroristického trestného činu

Článek 256 Propagace fašismu nebo jiného totalitního režimu

Článek 257. Rasismus

Článek 265 Poskytnutí nebo použití utajovaných informací s doložkou "tajné" nebo "přísně tajné"

Článek 266. Zveřejnění nebo použití informací získaných v souvislosti s výkonem úřední funkce nebo činnosti

Článek 267 Nezákonné získávání informací

Článek 268 Bránění oprávněné osobě v získání informací

Článek 268a. ničení, poškozování, mazání, pozměňování nebo bránění v přístupu k počítačovým datům.

Článek 269 Ničení, poškozování, mazání nebo pozměňování citlivých počítačových dat

Článek 269a. rušení provozu IT systému, datového komunikačního systému nebo sítě

Článek 269b. Nezákonná výroba, získávání, nakládání nebo poskytování počítačových programů

Článek 270. Padělání listiny a její použití jako pravé

Článek 270a. Falšování faktury a její použití pro ověření pravosti

Článek 271. Zkreslené údaje

Článek 271a. Zkreslení údajů na faktuře

Článek 272. Podvodné použití nepravdivých údajů v dokumentu

Článek 273. Použití nepravého dokladu Čl. 275.

Článek 275. Použití dokladu totožnosti jiné osoby

Článek 276. Zničení nebo zatajení dokumentu bez práva s ním nakládat

Článek 277a. Padělání faktury nebo použití padělané faktury s uvedením částky, na které je uveden majetek vysoké hodnoty.

Článek 278. Krádež

Článek 282. Loupež

Článek 284. Zpronevěra

Článek 285. Aktivace telefonních impulsů na cizí účet

Článek 286. Podvod

Článek 287. Počítačový podvod

Článek 291. Úmyslné přijetí

Článek 292. Neúmyslné přijetí

Článek 293. Počítačové zabavení majetku

Článek 296. Způsobení škody v obchodním styku

Článek 296a. Úplatkářství ve vedoucí pozici

Článek 297. Vymáhání úvěru

Článek 298. Vymáhání náhrady škody

Článek 299. Praní špinavých peněz

Článek 300. bránění uspokojení věřitele

Článek 303. Nevedení nebo nesprávné vedení obchodních záznamů

Článek 304. Využití smluvní strany

Článek 305. Zásah do veřejné zakázky

Článek 306. Odstraňování, padělání nebo pozměňování identifikačních značek

Článek 310. Padělání peněz, platebních prostředků nebo cenných papírů

Článek 311. Falšování informací při obchodování s cennými papíry

Článek 312. Oběh padělaných nebo pozměněných peněz, platebních prostředků nebo platebních dokladů

Článek 313. Falšování úředních značek cenných papírů

Článek 314. Falšování úředních značek za účelem jejich použití v obchodním styku

Článek 346. Násilí nebo nezákonná hrozba ze strany vojáka vůči jeho nadřízenému

Článek 347. Urážka nadřízeného vojákem

3.4. Hmotněprávní aspekty kybernetické trestné činnosti v Portugalsku

Under construction

4. Projevy kyberkriminality

Kyberkriminalita se typicky projevuje prostřednictvím kybernetických útoků, nicméně k úspěšnému uskutečnění řady útoků je třeba využít i ryze netechnické aspekty.

Určitá protiprávní jednání v kyberprostoru či jednání související s kyberkriminalitou je možné podřadit pod příslušná ustanovení platného trestního zákoníku, existují však určité typy jednání, jejichž označení za trestné činy může být podstatně obtížnější, či dokonce nemožné (v řadě případů se spíše jedná o pouze nemorální jednání).

Velmi často je kyberkriminalita považována za nový druh kriminality, nicméně značná část kyberkriminality využívá či přenáší notoricky známé druhy protiprávního jednání (např. podvody, porušování práv autorských, krádeže, šikanu aj.) do prostředí digitálního, ve kterém je lze páchat „lépe, rychleji, efektivněji" než ve světě reálném. Mezi ryze kybernetické útoky by pak bylo možné zařadit např. hacking, DoS a DDoS útoky, botnety aj.

Pro svět virtuální je příznačné, že většina uživatelů v něj má dle mého názoru až nepochopitelnou, téměř bezmeznou důvěru. Přičemž je třeba konstatovat, že svět virtuální se pro nás stává čím dál tím významnějším. Osobně mám pocit, že v případě využívání poskytovaných služeb na Internetu mnoho lidí přestane přemýšlet o možných rizicích či hrozbách. Primárně jsou uchváceni zdánlivě nekonečnými možnostmi „nových technologií"; jak jinak je pak možné vysvětlit si absenci základních obranných principů a mechanismů ve světě virtuálním, když ve světě reálném bychom se chovali zcela jinak. Jindy mi naopak uživatelé kyberprostoru svým chováním v něm připomínají *„Podivný případ Dr. Jekylla a pana Hyda"* [orig. Strange Case of Dr. Jekyll and Mr. Hyde - Robert Louise Stevenson (1886)]. Zdánlivě slušní lidé ve světě reálném, se v „pseudoanonymním" prostředí kyberprostoru projevují bez jakýchkoli legálních nebo morálních zábran. Je tak možné narazit například na případ soudce, jenž si stahuje „dětskou pornografii"[1], uživatele, kteří v reálném světě nikdy nic neukradli, ale ve světě virtuálním nemají problém krást[2], či porušovat jiná práva chráněná zákonem té které země.

K prognózám vývoje kyberkriminality se v minulosti vyjadřovala celá řada předních odborníků, z nichž si dovolím citovat zejména Schneiera, který v roce 2002 predikoval, že dalším velkým bezpečnostním trendem v Internetu bude zločin. *„Nepůjde o případy virů, trojských koní a DDoS útoků pro zábavu nebo možnost se vychloubat se svými schopnostmi. Půjde o skutečný zločin. V Internetu. Zločinci mají sklon zaostávat za vývojem technologií o pět, deset let, ale nakonec si uvědomí jejich možnosti. Tak jako Willie Sutton začal přepadat banky „protože tam byly peníze", tak moderní zločinci začnou útočit přes počítačové sítě. Stále více hodnot (finančních prostředků) je online, než v penězích reálných."*[3]

V roce 2007 představilo FBI statistiku, která porovnávala běžné „bankovní přepadení" (loupež) s jednáním, které má povahu phishingového útoku.[4]

Parametr	Průměrné ozbrojené přepadení	Průměrný kybernetický útok
Riziko	Pachatel riskuje, že bude zraněn či zabit.	Bez rizika fyzické újmy
Zisk	Průměrně 3 - 5 tisíc USD.	Průměrně 50 - 500 tisíc USD.
Pravděpodobnost dopadení	Dopadeno 50 - 60 % útočníků.	Dopadeno cca 10 % útočníků.
Pravděpodobnost odsouzení	Odsouzeno 95 % dopadených útočníků.	Z dopadených útočníků dojde k soudnímu projednávání pouze u 15 % útočníků a z nich je odsouzeno jen 50 %.
Trest	Průměrně 5 - 6 let, pokud pachatel při loupeži nikoho nezranil.	Průměrně 2 - 4 roky.

Goodman v roce 2012 ve vztahu k informačním a komunikačním technologiím uvádí, že *„schopnost jedince ovlivnit masy, právě díky těmto technologiím, roste exponenciálně. Exponenciálně roste jak v oblasti „dobrého, tak zlého účelu"*. Názorně tento růst prezentuje na vývoji zločinu loupeže, ke kterému v minulosti původně stačil nůž či pistole a de facto docházelo k loupežnému přepadení mezi jednotlivci či malými skupinami. *„K zásadní „inovaci" došlo v okamžiku loupežného přepadení celého vlaku, ve kterém cestovalo 200 lidí."* Internet umožňuje ještě výraznější rozsah útoku jedné osoby. Okradení velkého množství uživatelů dobře demonstruje případ Sony Playstation s přibližně 100 miliony poškozených osob. *„Kdy v historii lidstva mohl jedinec okrást 100 milionů lidí? Ale nejde jen o krádeže..."*[5]

V témže roce vystoupil s proslovem na RSA Cyber Security Conference (San Francisco, CA) ředitel FBI Robert S. Mueller, který mimo jiné ve své řeči uvedl: *„Jsem přesvědčen o tom, že existují pouze dva druhy společností: takové, do kterých se již hackeři nabourali, a ty, do nichž se teprve nabourají. A i tyto dvě skupiny se velmi rychle spojují v kategorii jedinou: společnosti, do jejichž systémů hackeři pronikli, a společnosti do nichž proniknou znovu."*[6]

V současnosti dochází ke stále většímu a masivnějšímu propojování různých počítačových systému do kyberprostoru, což de facto generuje přímou úměru spočívající v následujícím tvrzení: *„čím více je připojených zařízení, tím větší je jejich zranitelnost a tím větší bude počet útoků."* Jedno z grafických znázornění probíhajících útoků je možné nalézt na stránkách: http://map.norsecorp.com/#/; https://cybermap.kaspersky.com/; https://map.lookingglasscyber.com/ aj.

Domnívám se, že není možné pochybovat o tom, že kyberkriminalita je na vzestupu a představuje celosvětový problém. Různé statistiky uvádějí částečně rozdílné škody způsobené právě kyberkriminalitou, nic to však nemění na tom, že všechny do těchto škod započítávají škody primární (např. nefunkčnost počítačového systému, jeho části, nabízené služby, výpadek infrastruktury aj.) a škody sekundární (např. obnova systémů, záchrana dat, znovu

připojování koncových uživatelů aj.). Europol ve své zprávě z roku 2014[7] uvádí, že kyberkriminalita stojí globální ekonomiky přibližně 300 miliard $ ročně. Komunita útočníků se od masového rozšíření Internetu značně změnila. Primárně už se nejedná o individuality, které páchaly protiprávní jednání pro zábavu či překonávání překážek. V současnosti se zpravidla jedná o profesionály, kteří svoji činnost dělají s cílem profitovat a nezřídka jsou zapojeni do organizovaných skupin.

Tento posun je pochopitelný a neodmyslitelně spojený se třemi aspekty:

1) **Závislost společnosti na Internetu** (resp. nabízených službách, technologiích aj.),

2) **Kyberkriminalita se stala výnosným globálním businessem** [již první kybernetické útoky ukázaly možnosti zisku finančních prostředků, ať již přímo (odčerpáním financí), či zprostředkovaně (např. platbou za poškození služby jiné osoby)].

3) **Minimální gramotnost uživatelů**, kteří využívají informační a komunikační technologie (uživatel je typickým příkladem toho nejslabšího článku řetězu).

S rozvojem všemožných služeb postavených na principu as-a-service[8] vznikla i v prostředí kyberkriminality řada platforem (typicky undergroundových, darknet fór), kde jsou nabízeny služby, které je možné označit za **Crime-as-a-service** (cybercrime-as-a-service). Dochází tedy ke vzniku *„malware* či *underground economy“,* která poskytuje téměř jakémukoli uživateli prostředky ke spáchání kybernetických trestných činů. V rámci služby souhrnně označované crime-as-a-service jsou standardně nabízeny následující služby:

- *Research-as-a-service,*[9]
- *Crimeware-as-a-service,*[10]
- *Infrastructure-as-a-service,*[11]
- *Hacking-as-a-service,*[12]
- *Data-as-a-service,*[13]
- *Spam-as-a-service,*[14]
- *Ransomware-as-a-service* aj.

Výčet jednotlivých služeb není konečný a je možné konstatovat, že v rámci služby crime-as-a-service si lze objednat jakoukoli myslitelnou službu nebo komoditu, kterou lze v kyberprostoru využít či získat. Rozmach těchto negativních aktivit je přímo spojen i s fenoménem Internetu věcí (IoT), který propojuje zařízení (počítačové systémy) s Internetem, a představuje tak další výraznou hrozbu, která primárně spočívá v nerespektování některého ze základních principů bezpečnosti.

Řada výrobců či distributorů počítačových systémů, které je možné zařadit pod pojem IoT, neřeší otázku bezpečnosti (jejich cílem je co nejdříve na trh uvést a prodat co nejvíce zařízení, jež je možné označit za počítačový systém), čehož útočníci využívají.

Náklady spojené s vývojem v oblasti bezpečnosti jsou zpravidla nejnákladnější součástí vývoje, nicméně je to oblast, které je třeba se věnovat i s ohledem na již známé hrozby. Mezi ně například patří: nezabezpečený komunikační kanál u kardiostimulátoru[15]; auto či letadlo, jež lze ovládat na dálku[16]; chytrá domácnost či její součásti (lednice, kotel, zabezpečovací systém, televize aj.), jež lze ovládat na dálku[17] aj.

*„Jak asi dopadne svět, když máme **už tento rok** využívat 6,4 miliardy zařízení spadajících do IoT. Za další čtyři roky by to mělo být 20,8 miliardy zařízení. Řada z těchto zařízení navíc bude mít oproti běžnému životnímu cyklu mobilních telefonů, tabletů či laptopů podstatně delší životnost. Jak bude výrobce automobilů schopen chránit bezpečnost modelu z roku 2020 o deset let později? Nebo ledničky, která vám doma může stát i dobrých patnáct let? Jak dlouho trvalo, než se Microsoft naučil, jak aktualizovat vlastní operační systém?“*[18]

Schneier ve vztahu k datům uvádí, že útočníci s nimi mohou dělat v podstatě tři základní věci: krást je (narušení principu **Confidentiality** – důvěrnosti), měnit je (narušení principu **Integrity** – celistvosti) nebo zabraňovat vlastníkům v přístupu k nim (narušení principu **Availability** – dostupnosti). Schneier uvádí, že s nástupem IoT se právě poslední dva druhy útoků stanou extrémně účinné.[19]

V následující části představím některé útoky, ke kterým v prostředí kyberprostoru dochází. Nelze vymezit všechny útoky, ať již z důvodu rozsahu této publikace, či z důvodu nemožnosti popisu všech možných alternativních jednání subsumovatelných pod pojem kyberkriminalita. Pokud to bude možné, bude u konkrétního projevu kyberkriminality uvedena i případná trestněprávní kvalifikace takovéhoto jednání.

---

[1] *Judge, 69, who downloaded child porn facing 'catastrophic humiliation'.* [online]. [cit.1.9.2009]. Dostupné z: http://news.sciencemag.org/social-sciences/2015/02/facebook-will-soon-be-able-id-you-any-photo

[2] HILL, Kashmir. *These two Diablo III players stole virtual armor and gold — and got prosecuted IRL*. [online]. [cit.10.8.2015]. Dostupné z:

http://fusion.net/story/137157/two-diablo-iii-players-now-have-criminal-records-for-stealing-virtual-items-from-other-players/

[3] Blíže viz SCHNEIER, Bruce. *Crime: The Internet's Next Big Thing.* [online]. [cit.6.11.2007]. Dostupné z https://www.schneier.com/crypto-gram/archives/2002/1215.html

[4] JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007, s. 30

[5] Blíže viz GOODMAN, Marc. *A vision of crimes in the future.* [online]. [cit.13.11.2014]. Dostupné z: https://www.ted.com/talks/marc_goodman_a_vision_of_crimes_in_the_future#t-456071

[6] MUELLER, Robert. [online]. [cit.3.4.2013]. Dostupné z:

https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies

[7] Viz *The Internet Organised Crime Threat Assessment (iOCTA) 2014.* [online]. [cit.10.8.2015]. Dostupné z: https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta

[8]Jedná se o poskytování služeb typicky spojených s cloudovým řešením. Jako příklady je možné uvést: infrastructure-as-a-service; platform-as-a-service; Service-as-a-service; Security-as-a-service aj.

[9] Pod touto službou je možné si představit aktivity, které spočívají v odhalování nejrůznějších, dosud neznámých zranitelností cílového počítačového systému, či software (tyto zranitelnosti jsou známy jako zero-day vulnerabilities).

Vlastní činnost v rámci Research-as-a-service nemusí mít nutně povahu kriminálního či protiprávního jednání. Odhalování zranitelností a chyb se věnuje řada odborníků z IT bezpečnosti (např. penetrační testování aj.). Typicky jsou tyto služby poskytovány na základě smluvních podmínek mezi testovaným a testujícím, či za využití některé z okolností vylučujících protiprávnost.

[10] Služba crimeware-as-a-service nabízí celou řadu aktivit od prostého prodeje malware, přes jeho „úpravu na míru", dále pak dodávání exploitů (zranitelností) aj.

[11] Infrastructure-as-a-service pak představuje nabídku fyzických či virtuálních počítačových systémů (botnety, hostingové služby, pronájmy sítí aj.).

[12] Tato služba v sobě může zahrnovat prosté prolomení přístupových údajů k e-mailu, účtu na sociální síti aj. až po profesionální a sofistikované útoky na vybranou oběť. Do této oblasti pak může spadat např. i provedení útoků typu DoS a DDoS..

[13] Služba data-as-a-service nabízí nejžádanější komoditu, kterou jsou právě data. Konkrétně se jedná např. o: přístupové údaje (jméno a heslo) k různým účtům, kreditní karty, bankovní účty, kradené kreditní karty, ale i informace o osobách (bydliště, data narození, telefonní čísla, e-maily aj.).

[14] Z názvu vyplývá, že je možné si objednat a zaplatit spamovou kampaň.

[15] Srov. TAYLOR, Harriet. *How the „Internet of Things" could be fatal.* [online]. [cit.17.6.2016]. Dostupné z: http://www.cnbc.com/2016/03/04/how-the-internet-of-things-could-be-fatal.html

[16] Blíže viz GREENBERG, Andy. *Hackers remotely koll a Jeep on the highwaty – with me in it.* [online]. [cit.4.5.2016]. Dostupné z: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

V české verzi dostupné např. na: http://auto.idnes.cz/hackeri-unesli-jeep-dalkove-ovladani-auta-f1l-/automoto.aspx?c=A150723_135910_automoto_fdv

Blíže viz ZETTER, Kim. *Is It Possible for Passengers to Hack Commwrcial Aircraft?* [online]. [cit.5.5.2016]. Dostupné z: https://www.wired.com/2015/05/possible-passengers-hack-commercial-aircraft/

[17] Je tak možné např. obejít zabezpečení domácnosti; zvyšovat teplotu pomocí dálkově ovládaného termostatu a způsobit tak jinému škodu; objednat nesmyslné množství potravin prostřednictvím „chytré" lednice aj.

[18] DOČEKAL, Daniel. Bruce Schneier: *Internet věcí přinese útoky, které si neumíme představit.* [online]. [cit.10.8.2016]. Dostupné z: http://www.lupa.cz/clanky/bruce-schneier-internet-veci-prinese-utoky-ktere-si-neumime-predstavit/

[19] SCHNEIER, Bruce. *The Internet of Things Will Turn Large-Scale Hacks into a Real World Disasters.* [online]. [cit.10.8.2016]. Dostupné z: https://motherboard.vice.com/read/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster

4.1. Sociální inženýrství (Sociotechnika)

Sociální inženýrství nelze za každých okolností považovat přímo za kybernetický útok, nicméně je předpokladem pro to, aby byla řada kybernetických útoků úspěšná.

Pokud bychom chtěli definovat pojem sociální inženýrství, bylo by možné říci, že jde o ovlivňování, přesvědčování či manipulaci s lidmi s cílem je donutit provést určitou akci, či od nich získat informace, které by jinak neposkytli. Smyslem je v oběti navodit dojem, že situace, v níž se nachází, je jiná, než ve skutečnosti je. Zjednodušeněji by se dalo říci, že se jedná o „umění klamu", přičemž Mitnick rozlišuje dvě specializace v povolání umělce-manipulátora. *„Ten kdo mámí z lidí peníze je obyčejný podvodník, zatímco ten kdo využívá manipulace a přesvědčování vůči firmám – obvykle se záměrem získání informací – je sociotechnik."*[1]

Jsem přesvědčen, že toto tvrzení Mitnicka z roku 2003 by v současném digitálním světě neobstálo, neboť řada útočníků využívá techniky sociálního inženýrství pro to, aby získala právě informace či data a dále je využila například v rámci služby crime-as-a-service. Dále jsou tyto techniky využívány nejen vůči firmám, ale i vůči jednotlivcům. Vlastní útok primárně nemusí mít podobu podvodu, ale následně mohou být tyto informace prodány či zneužity k závažnějšímu útoku.

Hlavní myšlenkou sociálního inženýrství je nevyužívat různé ryze technické přístupy či nástroje například k prolomení hesla, když mnohem jednodušší je uvést oběť v omyl, ve kterém sama dobrovolně toto heslo prozradí. Nejslabším článkem bezpečnostního systému je a vždy bude člověk (uživatel). Jelikož na světě nemůže existovat počítačový systém, který by alespoň v nějaké fázi nebyl závislý na člověku (ať již jde o zprovoznění, nastavení, či údržbu počítačového systému), je nejjednodušší cestou získat potřebné informace právě od člověka.

Právě jednoduchost útoku zacíleného na nejslabší článek celého systému z něj zpravidla činí tu nejúčinnější formu. Sociální inženýrství se do popředí dostalo s kauzou Mitnicka[2], který je mnohými považován za hackera, avšak sám se spíše považuje za sociotechnika. Mitnick ve svých knihách[3] ukazuje, jak jednoduše lze získat informace, které jsou citlivé a představují bezpečnostní riziko pro jedince i organizace. V rámci slyšení před U.S. Senate Committee on Governmental Affairs[4], kde Mitnick vypovídal, jak získával hesla a citlivé informace k počítačovým systémům firem, do kterých pronikl, mimo jiné Mitnick uvedl: *„Představil jsem se jako někdo jiný a prostě jsem o ně požádal."*

Pro sociální inženýrství je jedním z klíčových faktorů zisk co největšího množství informací o cíli útoku (ať již počítačovém systému, právnické či fyzické osobě). Mnohdy dochází k dlouhodobému působení na klíčovou osobu a budování „důvěry" mezi útočníkem a obětí před vlastním útokem, přičemž útočník typicky využívá lidské neopatrnosti, důvěřivosti, ochoty pomoci jiným, lenosti, slabosti, strachu (např. aby se osoba nedostala do problémů), neodpovědnosti, hlouposti aj.

Výše uvedené lidské vlastnosti značně napomáhají útočníkovi realizovat jeho útok. Sami si položte otázku, jak moc si ověřujete protistranu například při telefonátu či komunikaci skrze ICT? Jak moc si prověřujete paměťová média (USB disky, paměťové karty aj.), které jste získali darem na prezentační akci?

Zejména v oblasti ICT je možné sledovat stále sofistikovanější a propracovanější útoky [např. kvalitně připravené podvodné e-maily, reálné instituce (použité jako domnělý odesílatel), přesměrování na podvodné stránky či instalace malware obsaženého v příloze dokumentu nebo na paměťovém médiu aj.].

Útoky sociálního inženýrství jsou zpravidla vedeny třemi způsoby, přičemž tyto způsoby jsou navzájem kombinovány:

1. **Sběr volně** (veřejně) **dostupných dat** o cíli útoku

2. **Fyzický útok** (útočník se například vydává za pracovníka servisní agentury – např. servis tiskáren, pracovník údržby aj.), při kterém se útočník snaží získat co nejvíce informací „zevnitř" společnosti, případně citlivé informace o jednotlivých pracovnících (včetně např. prohledávání odpadků aj.)

3. **Psychologický útok**

Mezi nejčastější metody útoků sociálního inženýrství lze zařadit:

1. **Podvodný e-mail** či **falešná webová stránka**

2. **Telefonický hovor**

3. **Útok „tváří v tvář"**

4. **Prohledávání odpadků** („Dumpster diving" a také „cezení dat")

5. **Prohledávání webu, sociálních sítí aj.** (jedná se o jednoduše dosažitelný otevřený zdroj dat pro útočníky sociálního inženýrství, který pomáhá zjistit, případně ověřit informace o potenciálním cíli). **Veřejné informace dostupné online** (např. životopisy, práce, teze, návrhy aj. uveřejněné na Internetu). **Výroční zprávy a jiné veřejně dostupné informace o společnosti**

6. **Doručení reklamních či jiných materiálů na CD, DVD či jiném paměťovém nosiči**

7. **Ponechání paměťového média** (USB aj.) **v zájmové oblasti** (např. firmě, u domu zaměstnance aj. toto médium pak typicky obsahuje malware)

8. **Nabídka vyzkoušení služby online** (např. nabídka cloudového úložiště, či některé zajímavé služby zdarma aj.)

9. **Dodávka či nalezení zařízení** (počítačového systému)

10. **Falešný servisní technik**

11. **Jiné**

Pokud jde o cíl útoků sociálního inženýrství v rámci organizace, pak se možnými cíli mohou stát například:

- Řídící pozice,
- IT oddělení,
- pracovníci help desků,
- recepční (sekretariáty),
- bezpečnostní pracovníci,
- správa budov,
- úklid aj.

Sociotechnik je schopen díky svým schopnostem manipulovat s lidmi, nicméně prostá manipulace není v některých případech dostačující a je třeba propojit tyto informace s technickými znalostmi v oblasti ICT.

Na závěr této kapitoly uvádím příklad, na němž Mitnick demonstruje právě propojení sociálních technik se znalostmi ICT:[5]

Mladý hacker, kterému budu říkat Ivan Peters, si dal za cíl získat zdrojový kód nové hry. Bez potíží se dostal do firemní sítě WAN, protože jeho hackerský kolega se už dříve dokázal nabourat na jeden z jejich webových serverů. Po odhalení jisté slabiny v softwaru div že nespadl ze židle. Ukázalo se, že systém používal tzv. *dual homing,* což znamená, že měl odtud přístup i do vnitřní sítě.

Avšak po připojení stál Ivan před podobným problémem, před jakým stojí turista v Louvre, který chce najít portrét Mony Lisy. Bez průvodce by se tam mohl motat celé týdny. Byla to globální korporace se stovkami kanceláří a tisíci serverů, která ve své síti nezveřejňovala indexy vývojářských systémů nebo jiné průvodcovské služby po svých datech. Místo toho, aby k nalezení serveru, na který se potřeboval dostat, použil technologické metody, využil metodu sociotechnickou. Uskutečnil několik telefonátů na základě postupů v této knize už popsaných. Nejprve zatelefonoval na technickou pomoc oddělení informatiky, představil se jako zaměstnanec firmy a řekl, že by rád probral jistý problém spojený s rozhraním produktu, na kterém pracovala jeho skupina. Požádal o telefonní číslo na šéfa projektů ve skupině programátorů, kteří se zabývali hrami. Potom zavolal na toto číslo a předstíral, že je pracovníkem oddělení Informatiky. *„Ještě dnes večer,"* řekl, *„budeme měnit router a chceme se ujistit, že lidé z vaší skupiny neztratí spojení se serverem. Který server používáte?"* Síť byla neustále vylepšována a sdělení jména serveru nemůže ničemu vadit, že? Vždyť je přece chráněn heslem a samotná znalost jména nikomu nic nepřinese. A tak šéf projektů uvedl jméno serveru. Ani se nepokusil o zpětné zavolání a ověření této historky nebo alespoň o zapsání jména a telefonního čísla volajícího. Prostě sdělil jména serverů: ATM5 a ATM6.

Nyní se Ivan vrátil k technologickým metodám, aby získal autentikační informace. Ve většině případů je prvním krokem identifikace účtu se snadným heslem, které dovolí získat v systému první opěrný bod. Pokud se útočník pokouší za pomoci hackerských nástrojů vzdáleně identifikovat hesla, vyžaduje to být po dlouhé hodiny připojen k firemní síti.

Objevuje se tu nebezpečí: čím déle bude připojen k síti, tím větší je riziko jeho odhalení a dopadení. Nejprve použil Ivan enumeraci, která umožňuje odhalit podrobnost o systému. Jako obvykle je možné vhodné nástroje nalézt na Internetu, *(http://mtslenth.0catch.com*). Ivan našel na webu několik volně dostupných hackerských nástrojů, které mu dovolily proces zautomatizovat a vyhnout se tak ruční práci, která by prodlužovala čas operace, a tím by zvětšovala i riziko dopadení. Věděl, že firma většinou používá servery na platformě Windows a stáhl si program NTBEnum — enumerační nástroj[6] NetBIOS (basic input/output system). Zadal IP adresu serveru ATM5 a spustil program. Nástroj dokázal identifikovat několik existujících kont na serveru.

Po identifikaci existujících kont stejný program umožnil spuštění slovníkového útoku. Slovníkový útok je dobře známý lidem zabývajícím se bezpečností počítačových systémů a samozřejmě i hackerům. Ostatní lidi fakt, že je něco takového vůbec možné, šokuje. Tento útok má za cíl zjištění hesel uživatelů pomocí obecně užívaných slov. Všichni jsme v některých věcech líní, ale nikdy mne nepřestane udivovat, že při výběru hesla má lidská kreativita a představivost prázdniny. Většina z nás chce mít heslo, které nás ochrání, ale zároveň je lehké si ho pamatovat. Obvykle to znamená použití nějakého nám blízkého slova. Mohou to být například naše iniciály, druhé jméno, přezdívka, jméno manžela, název oblíbené písničky, filmu či značky piva. Dále pak jméno ulice či města, kde bydlíme, značka auta, kterým jezdíme, oblíbené prázdninové místo nebo jméno potoka, kde nejlépe berou pstruzi. Vidíme to pravidlo? Většinou jsou to jména nebo výrazy, které lze najít ve slovníku. Slovníkový útok zkouší postupně výrazy ze slovníku jako heslo jednoho či více uživatelů.

Ivan provedl slovníkový útok ve třech fázích. V první fázi seznam 800 nejčastěji používaných hesel. Seznam obsahuje taková jako *secret, work* nebo *password* (tedy *tajné, práce, heslo*). Kromě toho program tvořil permutace těchto výrazů s doplněnými číslicemi nebo s číslem aktuálního měsíce. Program zkoušel každé heslo na všech nalezených účtech v systému. Bez výsledku. Ve druhé fázi si otevřel stránku vyhledávače Google a zadal výraz *„wordlists dictionaries*" a našel tisíce stran obsahující seznamy slov a anglické i jiné slovníky. Stáhl si celý elektronický anglický slovník. Doplnil ho o několik seznamů výrazů, které našel vyhledávač. Ivan si vybral adresu *www.outpost9.com/files/Wordlists.html*. Z této stránky se mu podařilo stáhnout (úplně zadarmo) sadu souborů obsahující příjmení, neobvyklá jména, jména a výrazy spojené s politikou, jména herců a slova a jména pocházející z Bible. Jiná stránka se seznamy výrazů je dostupná na univerzitě v Oxfordu na adrese *ftp://ftp.ox.ac.uk/pub/wordlists* . Na jiných adresách můžeme najít seznamy se jmény postav z animovaných filmů, citáty ze Shakespeara, z Odyssey, z Tolkiena i Hvězdných válek a také slova spojená s vědou, náboženstvím atd. (Jedna internetová firma prodává seznam obsahující 4,4 milionu slov a jmen za pouhých 20 dolarů.) Atakující program může být zkonfigurován i tak, aby tvořil na základě výrazů ze slovníku anagramy - to je další oblíbená metoda uživatelů, která má zvětšit jejich bezpečnost.

Když si Ivan vybral seznam, který použije a spustil program, přepnul ho do automatického režimu a mohl se tak věnovat něčemu jinému. Člověk by si myslel, že takový útok dá útočníkovi čas na delší šlofíček a dokonce, že až se vzbudí, bude pokrok nevelký. Ve skutečnosti může být - v závislosti na druhu napadeného systému, konfiguraci bezpečnostních systémů a rychlosti připojení - plná slovní zásoba z anglického slovníku otestována za 30 minut! Během útoku zapnul Ivan druhý počítač a rozběhl podobný útok na druhý server, který používala skupina programátorů, ATM6. O dvacet minut později se podařilo něco, co se většině lidí zdá nemožné: prolomit heslo a odhalit, že jeden z uživatelů si zvolil heslo *„Frodo*", jméno jednoho z hobitů, hrdiny Pána prstenů. S heslem v ruce se Ivan mohl připojit k serveru ATM6. Čekala tam na něho dobrá a špatná zpráva. Dobrá, že konto, na které se naboural, mělo administrátorská práva. A špatná, že tam nikde nemohl najít zdrojový kód hry. Zřejmě byl na druhém serveru, ATM5, který se

slovníkovému útoku ubránil. Ivan však neházel flintu do žita - stále ještě měl v zásobě pár triků. V některých operačních systémech Windows a UNIX jsou zašifrovaná hesla přístupná každému, kdo má přístup na počítač, kde jsou umístěná. Důvodem je fakt, že zakódovaná hesla nelze dekódovat zpět a tedy není důvod je chránit. Tato teorie je mylná. Pomocí dalšího nástroje dostupného na síti, *pwdump3*, si stáhl zakódovaná hesla ze serveru ATM6. Typický soubor se zakódovanými hesly vypadá takto:

Administrator: 500:95E4321A38AD8D6AB75E0C8D76954A50:

2E48927AQB04F3BFB341E266D6L

akasper:1110:5A8D7E9E3C3954F642C5C736306CBFEF:393CE7F90A8357F157873D72D

digger:1111:5D15COD58D0216C525AD3B83FA6627C7:17AD564144308B42B8403D01AE256

555

ellgan:1112:2017DA45D8O1383EFF17365FAF1FFE89:07AEC950C22CBB9C2C734EB89j1

tafeeck:1115:9F5890B3FECCAB7EAAD3B435B51404EE:1F0115A728447212FC05E1D208203

35

vkantar;1116:81A6A5D035596E7DAAD3B435B51404EE:B933D36DD12258946FCC7BD153F1

CD6

vwallwick:1119:25904EC665BA30F44494F42E1054F192:15B2B7953FB632907455D2706A432

mmcdonald: 1121:

A4AED098D29A3217AAD3B435B51404EE:40670F936B79C2ED522F5ECA939c

kworkman:1141:C5C598AF45768635AAD3B435B51404EE:DEC8E827A121273EF084CDBF5F

D192

Když měl soubor u sebe na počítači, použil Ivan další nástroj, který prováděl tzv. *útok hrubou silou*.[7] Ten zkouší všechny kombinace alfanumerických a většiny speciálních znaků.

Ivan použil nástroj *L0phtcrack3* (čti loft-crack; je dostupný na adrese *www.atstake.com*; jiný zdroj vynikajících nástrojů na hádání hesel je *www.elcomsoft.com*). Správci používají L0phtcrack3 na vyhledávání *„slabých"* hesel a hackeři na jejich proražení. L0phtcrack3 umožňuje zkoušet hesla s kombinacemi písmen, číslic a většiny symbolů včetně @#$%^&. Systematicky testuje všechny možné kombinace většiny znaků. (Pokud jsou však v hesle použity neviditelné znaky, L0phtcrack3 nebude schopný heslo odhalit.) Tento program pracuje s neuvěřitelnou rychlostí, která může na počítači s frekvencí procesoru 1 GHz dosáhnout hodnoty 2,8 milionu pokusu za sekundu. Dokonce i při této rychlosti může, pokud správce dobře zkonfiguroval systém Windows (tj. vypnul používání hašování LANMAN), prolomení hesla zabrat hodně času. Z tohoto důvodu si útočník často stahuje soubory s hesly na svůj počítač a spouští útok u sebe, aby neriskoval odhalení během dlouho udržovaného spojení. Ivan nemusel čekat dlouho.

O několik hodin později našel program hesla všech členů skupiny programátorů. Byla to však hesla uživatelů na ATM6, kde nebyl zdrojový kód. Co teď? Stále nebyl schopen získat hesla umožňující přístup k serveru ATM5. Jako hacker si uvědomoval zlozvyky většiny uživatelů a došel k závěru, že si někdo z členů týmu mohl vybrat stejné heslo na obou serverech. A bylo to tak. Jeden z programátorů měl heslo *gamers* jak na ATM5, tak i na ATM6. Před Ivanem se otevřely dveře k hledání zdrojového kódu.

Když ho našel a stáhl si celý strom, učinil ještě jednu pro hackera typickou věc. Změnil heslo na spícím kontě s administrátorskými právy, čistě pro případ, že by se sem chtěl později vrátit a stáhnout si novou verzi programu.

K redukci rizik sociálního inženýrství je nezbytné zvyšovat povědomí o možných hrozbách nejen v rámci organizace, ale v rámci celé společnosti. Jak jsem již uvedl dříve, sociální inženýrství pomáhá uskutečnit útok, přičemž je zcela na útočníkovi, aby určil, kdo bude jeho cílem. Pro útočníka je mnohem snazší zaměřit svůj útok na masy nezkušených a neznalých lidí, než na relativně dobře chráněnou společnost.

---

[1] MITNICK, Kevin D. a William L. SIMON. *Umění klamu*. Gliwice: Helion, 2003. ISBN 83-7361-210-6. s. 6

[2] Blíže viz např. *Kevin Mitnick Case: 1999.* [online]. [cit.2.11.2011]. Dostupné z: http://www.encyclopedia.com/doc/1G2-3498200381.html

[3] Blíže viz:

MITNICK, Kevin D. a William L., SIMON. *Umění klamu*. Gliwice: Helion, 2003. ISBN 83-7361-210-6.

MITNICK, Kevin D. *The art of intrusion: the real stories behind the exploits of hackers, intruders & deceivers*. Indianapolis: Wiley, c2006. ISBN 0-471-78266-1.

MITNICK, Kevin D. a William L., SIMON. *Ghost in the wires: my adventures as the world's most wanted hacker*. New York: Little, Brown & Co, 2012. ISBN 9780316037723.

[4] *The testimony of an ex-hacker.* [online]. [cit.26.9.2008]. Dostupné z: http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/testimony.html

[5] Příklad doslova citován z: MITNICK, Kevin D. a William L. SIMON. *Umění klamu*. Gliwice: Helion, 2003. ISBN 83-7361-210-6, s. 127-130

[6] **Enumerace -** proces odhalující služby dostupné na daném serveru, jeho operační systém a názvy uživatelských kont, které mají přístup do systému.

[7] **Útok hrubou silou (Brute force attack)** - strategie odhalování hesel, která spočívá v testování všech možných kombinací alfanumerických i speciálních znaků.

4.2. Botnet

Botnet lze jednoduše definovat jako síť softwarově propojených botů[1], které provádí činnost na základě příkazu „vlastníka“ (resp. správce) této sítě. Takto postavená síť může být použita k legální činnosti (např. distribuované výpočty), nebo k činnosti nelegální (viz dále).

Právě distribuované výpočty, de facto nechtěně, vnukly zločincům myšlenku na vybudování botnetů tak, jak je vnímáme v současnosti. Z upoutávky na distribuované výpočty uvádím: *„**většina počítačů na světě využívá svůj plný výpočetní potenciál jen velice malou část své provozní doby**, ale jejich spotřeba elektřiny je jen o málo nižší než kdyby byly vytíženy naplno. J**e obrovská škoda tohoto lenošení počítače nevyužít, a málokdo si uvědomuje, kolik takového nevyužitého výkonu na světě vlastně je**... V distribuovaných výpočtech platí do písmene pořekadlo **„Nemusí pršet, stačí když kape“ a zde kape z milionů obyčejných počítačů na světě takový výkon, který převyšuje několikanásobně výkon i těch největších superpočítačů světa...** Zapojení do jakéhokoliv projektu distribuovaného výpočtu spočívá pouze v instalaci klienta a ten už většinou dokáže provádět veškeré potřebné činnosti a starat se o konkrétní aplikace...Většina projektů funguje tak, že celková práce je rozdělena na spoustu dílků a ty jsou následně rozesílány na jednotlivé počítače, které si o ně řeknou. Po zpracování každého dílku jednotlivé počítače samy odešlou výsledná data zpět do centra projektu a tam dojde ke spojení výsledků opět do jednoho celku.“*[2]

Vlastní idea distribuce zdrojů, respektive využití malého výpočetního výkonu jiných počítačových systémů například pro počítání složitých matematických algoritmů aj. rozhodně není špatná a je mnohem efektivnější, než využívání a budování „superpočítačů“. Nicméně jako lidé jsme značně vynalézaví, a tak bylo nasnadě, že tato myšlenka bude využita i k jiným než nezištným či prospěšným účelům. Možnost distribuce různých úloh mezi různě geograficky umístěné počítače byla a je pro útočníky lákavá.

Současný počítačový systém např. v podobě mailserveru nemá problém odeslat desítky milionů či miliardy e-mailových zpráv denně. Pokud se uživatel rozhodne tento systém využívat například k šíření Spamu, bude tento počítačový systém (dohledatelný podle identifikátorů jako je IP adresa) tuto činnost vykonávat pouze po velmi krátkou dobu, neboť bude velmi brzy zablokován ISP (např. z důvodu nelegitimního či nadměrného provozu v síti, který je možné označit za Spam), jeho adresa se objeví na „blacklistech“ a na základě této informace bude blokován provoz (např. odchozí pošta). Pokud však útočník využije distribuovaný výkon v podobě sítě botnet, bude mít k dispozici tisíce až stovky tisíc počítačů, z nichž každý odešle část zpráv (např. 1000-2000 zpráv denně). Takovýto provoz pak nebude považován za problematický a nebude zastaven.

Pro **botnet** je typické, že **pokud se podaří infikovat cílový počítačový systém, připojí se tento systém**, který je nazýván „zombie“ či „bot“ (zotročený počítačový systém) **k centrálnímu řídícímu serveru** [označovanému jako command-and-control server (C&C)]. **Kontrolu nad celým tímto systémem** (obsahujícím zombie a C&C) **má útočník** (označován jako botmaster či botherder), **jenž řídí boty prostřednictvím C&C serveru**.[3]

Pro botnet jsou charakteristické (nezbytné) následující prvky:

1. **Command-and-control infrastructure (C&C)**

Jedná se o infrastrukturu, která se skládá z řídícího prvku (či prvků) a botů (ovládaných počítačových systémů).

2. **Instalace a ovládání botu**

Nejčastěji se jedná o malware, který je prostřednictvím sítě botnet či jiným způsobem šířen. Primárním cílem takovéhoto malware je zapojit další počítačové systémy do botnetu. Malware využívá různé zranitelnosti počítačových systémů.

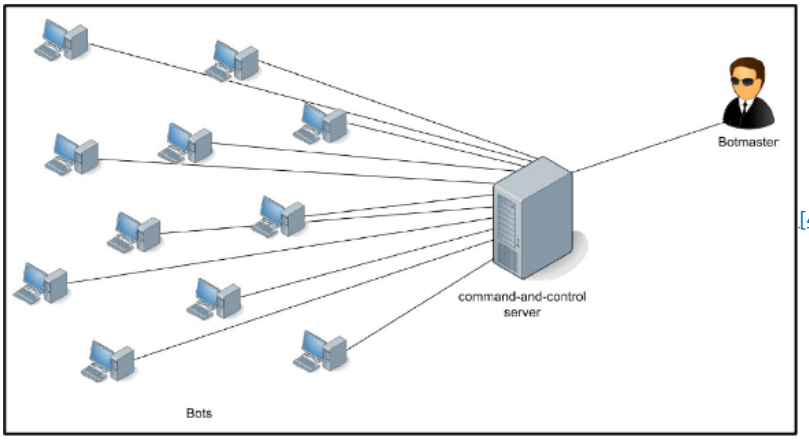
3. **Řízení** (ovládání) **botů zkrze C&C infrastrukturu**

Bot je software, který funguje skrytě a ke komunikaci s C&C serverem používá běžné komunikační kanály (IRC, IM, RFC 1459 aj.). Noví boti se snaží získat co nejvíce informací ze svého okolí a propagovat se do dalších počítačových systémů.

Na základě architektury se standardně rozlišují botnety s:

1. **Centralizovanou architekturou**

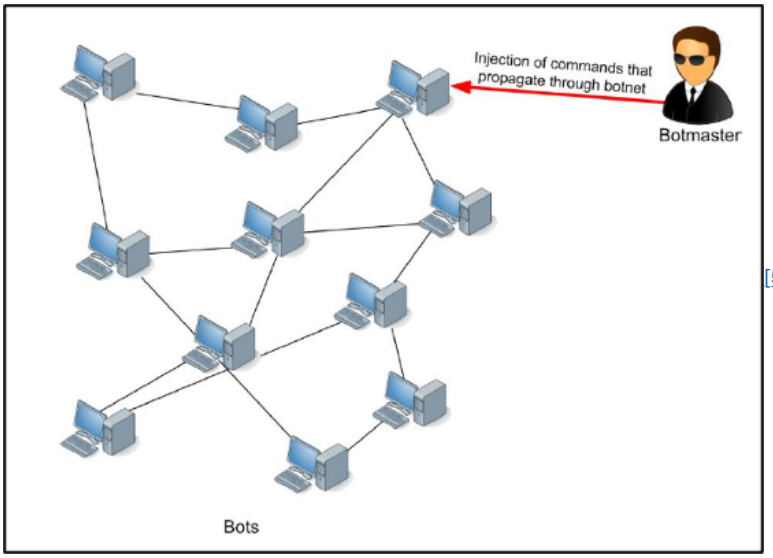
Tato architektura je typicky postavena na principu komunikace klient-server. Koncové počítačové systémy (zombie/boti) komunikují přímo s C&C serverem (centrálním řídícím prvkem) a plní instrukce a využívají zdroje z tohoto serveru.



[4]

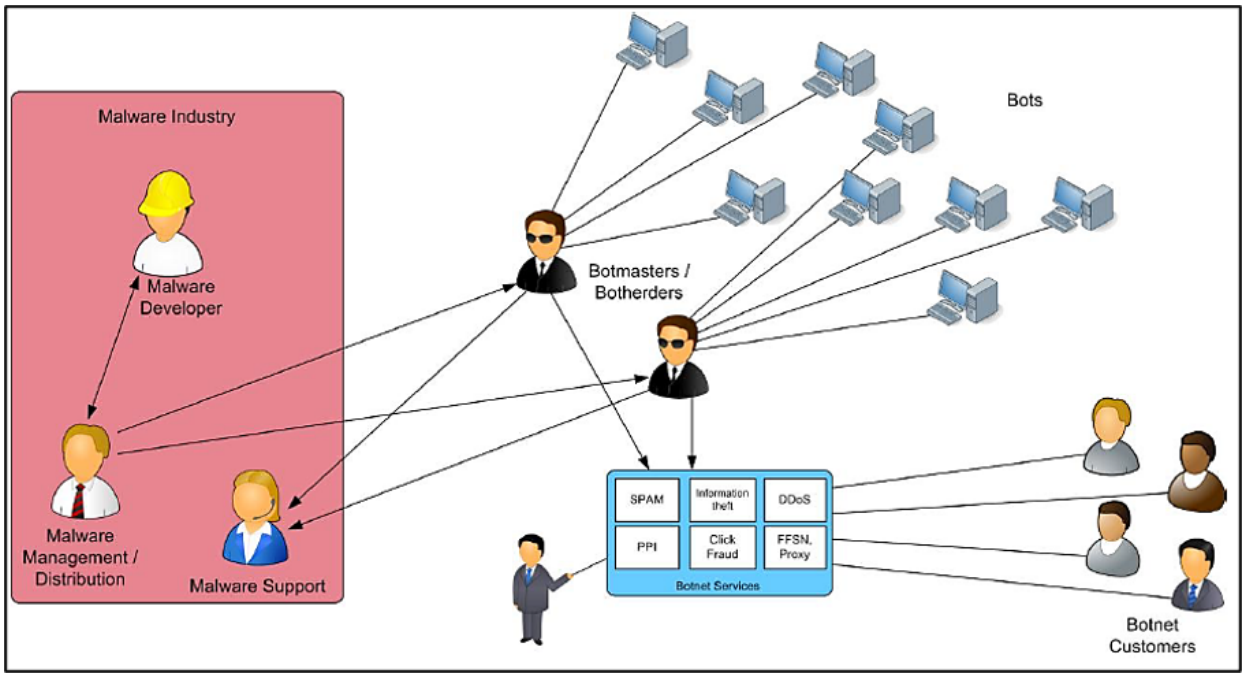
2. **Decentralizovanou architekturou**

Typicky je vybudovaná na Peer-to-peer (P2P) architektuře. Tato architektura umožňuje sdílení zdrojů a příkazů v rámci P2P sítě. Chybí zde centrální řídící prvek v „klasické“ podobě, díky čemuž je tento systém odolnější proti snaze o převzetí kontroly prostřednictvím tohoto řídícího prvku.



[5]

Botnety je možné využít k řadě činností, avšak v popředí je především finanční zisk, který spočívá jednak v generování vlastních útoků (např. ransomware, phishing, rozesílání spamu, krádežím informací, DDoS aj.), tak v pronájmu svých služeb či celého botnetu klientům. Díky výše popsanému je možné botnet zařadit do struktury **crime-as-a-service** (kde je nabízena služba: **botnet-as-a-service**), či do malware economy[6], kde představuje základní technickou platformu, nezbytnou pro provedení celé řady kybernetických útoků.



Malware economy

Počítačový systém, který se stane součástí botnetu, je pak typicky využit pro některou z činností popsaných v následující tabulce. Je třeba uvést, že uvedené útoky jsou zpravidla vzájemně kombinovány či distribuovány v rámci botnetu s ohledem na jeho vytíženost, poptávku „zákazníků“ atp.

Odesílání	Identity Theft	DoS útoky	Click Fraud
- spamu - phishingu - malware - adware - spyware	Dochází k získávání a odesílání (zpět útočníkovi) osobních a citlivých dat a informací. - Přístupové údaje k účtům - Přístupové údaje k e-mailům, sociálním sítím aj. - jiná data či informace, které mohou být útočníkem využity, či prodány	Spouštění DoS útoku vůči cíli (počítačovému systému) určenému botmasterem.	Počítačový systém zobrazuje (případě kliká) na reklamní odkazy na stránkách bez vědomí uživatele. Vytváří se tak dojem, že stránky mají návštěvnost a inzerenti přicházejí o peníze.[7]

V níže uvedené tabulce shrnuji seznam některých známých botnetů[8]:

Datum vytvoření	Datum ukončení	Jméno	Předpokládaný počet botů	Počet spamu v miliardách	Alias (známý též jako)	Další informace

				za den		
2002						
	2011	Coreflood	2,300,000			Backdoor. Sběr osobních a citlivých informací.
2004						
		Bagle	230,000[16]	5.7	Beagle, Mitglieder, Lodeight	Masivní rozesílání spamu. Určený pro počítačové systémy s OS Windows.
		Marina Botnet	6,215,000[16]	92	Damon Briant, BOB.dc, Cotmonger, Hacktool.Spammer, Kraken	
		Torpig	180,000[17]		Sinowal, Anserin	Rozesílání malware a sběr citlivých a osobních dat. Určený pro počítačové systémy s OS Windows.
		Storm	160,000[18]	3	Nuwar, Peacomm, Zhelatin	Rozesílání spamu. Určený pro počítačové systémy s OS Windows.
2006						
	Březen 2011	Rustock	150,000[19]	30	RKRustok, Costrat	Rozesílání spamu. Schopnost odeslání až 25 000 spamových zpráv/hodina z jednoho počítač. Aktivní na OS Windows.
		Donbot	125,000[20]	0.8	Buzus, Bachsoy	Rozesílání především farmaceutického spamu.
2007						
		Cutwail	1,500,000[21]	74	Pandex, Mutant (related to: Wigon, Pushdo)	Rozesílání spamu. Standardně používí Trojského koně Pushdo, aby infikoval počítačový systém. Aktivní na OS Windows.
		Akbot	1,300,000[22]			Backdoor, umožňující převzetí kontroly nad nakaženým počítačem. Po instalaci sbíral data, zastavoval procesy, či spouštěl DDoS útoky.
Březen 2007	Listopad 2008	Srizbi	450,000[23]	60	Cbeplay, Exchanger	Primárně rozesílání spamu. K nakažení počítačových systémů byl využíván Srizbi trojan.
		Lethic	260,000[16]	2	none	Rozesílání především farmaceutického spamu.
Září 2007		dBot	10,000+ (Europe)		dentaoBot, d-net, SDBOT	
		Xarvester	10,000[16]	0.15	RIsloup, Pixoliz	Rozesílání spamu.

2008						
		Sality	1,000,000[24]		Sector, Kuku	Skupina malware. Počítačové systémy nakažené Sality komunikují skrze P2P. Činnost spočívá v: rozesílání spamu, sběr citlivých dat, napadání webových serverů, provádění distribuovaných výpočtů (např. pro prolamování hesel – password cracking aj.). Aktivní na OS Windows.
Duben 2008		Kraken	495,000[33]	9	Kracken	Rozesílání malware. Zapojení dalších počítačů do botnetu.
	Prosinec 2009	Mariposa	12,000,000[25]			Botnet primárně zapojený do útoků typu scam a DDoS. **Jednalo se o jeden z největších botnetů vůbec.**
Listopad 2008		Conficker	10,500,000+[26]	10	DownUp, DownAndUp, DownAdUp, Kido	Worm útočící na počítačové systémy s OS Windows. Chyby tohoto OS byly využity k dalšímu rozšiřování botnetu.
Listopad 2008	Březen 2010	Waledac	80,000[27]	1.5	Waled, Waledpak	Rozesílání spamu a šíření malware. Ukončen akcí společnosti Microsoft.
		Maazben	50,000[16]	0.5	None	Rozesílání spamu, malware, scamu, phishingu.
		OnewordSub	40,000[28]	1.8		
		Gheg	30,000[16]	0.24	Tofsee, Mondera	
		Nucrypt	20,000[28]	5	Loosky, Locksky	
		Wopla	20,000[28]	0.6	Pokier, Slogger, Cryptic	
		Asprox	15,000[29]		Danmec, Hydraflux	Phishingové útoky, SQL injections, šíření malware.
		Spamthru	12,000[28]	0.35	Spam-DComServ, Covesmer, Xmiler	Používání P2P
	19.7.2012	Grum	560,000[31]	39.9	Tedroo	Rozesílání především farmaceutického spamu.
		Gumblar				
2009						
Květen 2009	Listopad 2010	BredoLab	30,000,000[30]	3.6	Oficla	Rozesílání spamu. Ukončen společnou akcí nizozemské policie,

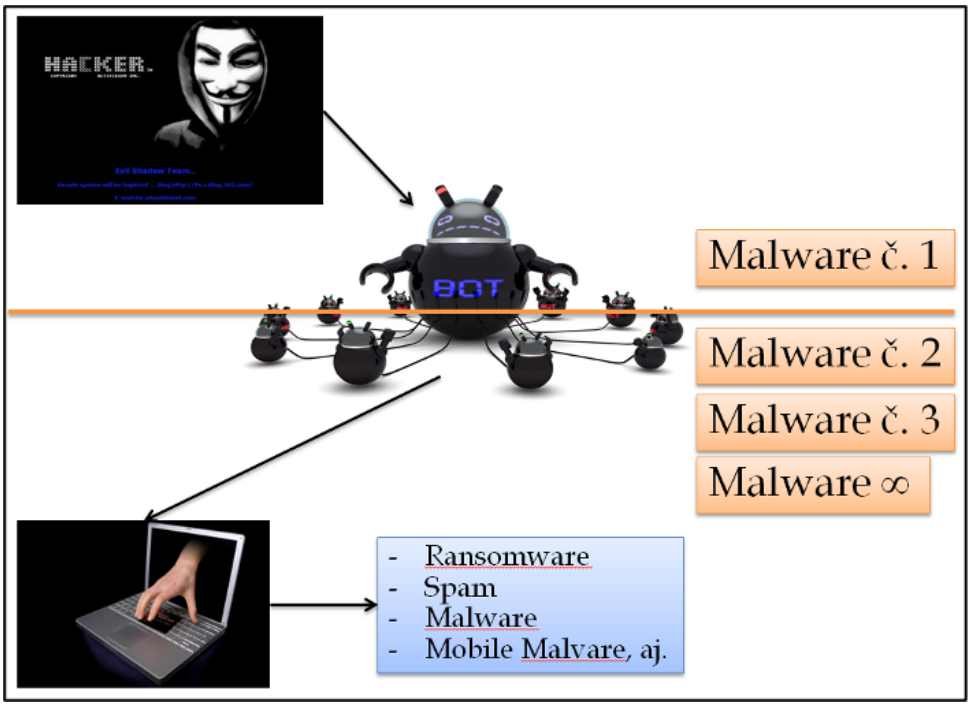
						Govcert NL, Europolu. Kasperky Lab aj. **Zřejmě největší známý botnet.**
	Listopad 2009	Mega-D	509,000[32]	10	Ozdok	Rozesílání spamu.
Srpen 2009		Festi	250,000[34]	2.25	Spamnost	Rozesílání spamu a provádění DDoS útoků.
2010						
Leden 2010		LowSec	11,000+[16]	0.5	LowSecurity, FreeMoney, Ring0.Tools	
		TDL4	4,500,000[35]		TDSS, Alureon	
		Zeus	3,600,000 (US only)[36]		Zbot, PRG, Wsnpoem, Gorhax, Kneber	Zaměřen na aktivity spojené s krádežemi informací k bankovním účtům. Instaloval i Cryptolocker Ransomware aj. Aktivní na OS Windows.
	(Several: 2011, 2012)	Kelihos	300,000+	4	Hlux	Převážně zapojený do krádeží Bitcoinů a rozesílání spamu.
2011						
	2015-02	Ramnit	3,000,000[37]			Worm útočící na počítačové systémy s OS Windows. Ukončen společnou akcí Europolu a Symantec.
		Zero Access	2,000,000		Max++ Sirefef	Botnet využitý převážně k těžení bitcoinů a click fraudu. Aktivní na OS Windows.
2012						
		Chameleon	120,000		None	Click Fraud
		Nitol				Botnet zapojený do šíření malware a DDoS útoků. Většina zombie (až 85 %) se nachází v Číně. Botnet klient byl nalezen v počítačových systémech dodaných přímo z výroby.
2013						
		Boatnet	500+ server computers	0.01	YOLOBotnet	
		Zer0n3t	200+ server computers	4	FiberOptck, OptckFiber, Fib3rl0g1c	
2014						
		Semalt	300,000+		Soundfrost	Rozesílání spamu.
		Necurs	6,000,000			
2016						

		Mirai	380,000			DDoS.Rozesílání spamu.
		Methbot	6,000 domains and 250,267 distinct URLs			
2018						
		3ve	1.7 million computers and a large number of servers			Money theft.

Do sítě botnet je de facto možné zapojit jakýkoli počítačový systém. Mimo jiné se jedná i o systémy, které splňují podmínky IoT (Internet of Things). V roce 2014 byl zaznamenán případ, kdy součástí botnetu byla lednice, jež rozeslala více než 750 000 e-mailů, které měly povahu spamu.[9]

Ze studie Nigama vyplývá[10], že existují desítky botnetů přímo vytvářených a primárně zaměřených na počítačové systémy, které můžeme označit jako mobilní zařízení (např. smartphone, tablet aj.). Díky instalaci aplikací z neznámých zdrojů a značné absenci antivirových produktů na mobilních zařízeních uživatelů je také mnohem snadnější nainstalovat malware do těchto mobilních zařízení, a tím nad nimi získat kontrolu. Tato zařízení jsou v současnosti svým výkonem schopna zcela splnit požadavky botmastera na chod botnetu, respektive na úkoly kladené na „zombie".

Nejen v případě botnetů slouží malware jako prostředek k získání přístupu, ovládání a dalšímu šíření malware či jiným úkolům na základě pokynů útočníka, nicméně pokud je v současnosti na uživatelův počítačový systém infikován malware, existuje vysoká pravděpodobnost, že se zároveň stal součástí botnetu. Útočník (botmaster) do počítačového systému (zombie) nainstaluje malware, který mu umožňuje manipulaci s počítačovým systémem na dálku (Malware č. 1 – přičemž tento malware ponechává kontrolu botmasterovi i v případě například pronájmu části nebo celého botnetu.). Teprve poté dochází k instalaci dalšího škodlivého software (Malware **2**. až Malware **∞**), který má plnit jiné úkoly (např. rozesílání spamu, sběr dat, vydírání pomocí Ransomware aj.). Celou tuto strukturu je možné znázornit následovně:



Malware instalovaný do počítačového systému zapojeného do sítě botnet

Z pohledu práva je možné konstatovat, že botnety představují celé sítě infikovaných počítačových systémů, nad kterými do určité míry neoprávněně převzala kontrolu třetí osoba, a to bez vědomí oprávněných uživatelů. Takto infikované systémy slouží nejčastěji jako základna pro anonymní připojování útočníka k Internetu, k zasílání škodlivých programů, uskutečňování útoků na další cíle, realizaci DoS útoků, šíření spamu, krádežím identit či jiným kybernetickým útokům.

Možnosti trestněprávního postihu v ČR

Pokud jde o vlastní činnost útočníka, která spočívá v instalaci malware pro následné ovládnutí počítačového systému, je možné toto jednání posoudit dle **§ 230** TZK (Neoprávněný přístup k počítačovému systému a nosiči informací). Pokud by útočník malware vložil do počítačového systému v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch, mohlo by být jeho jednání kvalifikováno dle § 230 odst. 2 písm. d) TZK.

Lze tvrdit, že se jedná i o neoprávněné užívání cizí věci (neboť předmětný počítačový systém je v těchto případech věcí cizí) dle **§ 207 odst. 1 al. 1** TZK. Užití § 207 odst. 1 al. 2 TZK[11] může být značně problematické, neboť je rozhodující intenzita zásahu a užívání počítačového systému. Na základě této míry intenzity by bylo případně možné vyčíslit vzniklou škodu, jakožto vyjádření amortizace v čase užívání. Bohužel za použití tohoto výpočtu zpravidla nedojde ke způsobení škody nikoli malé.

Vlastní ochrana před zapojováním a využíváním počítačů v rámci sítě botnet může mít dvě roviny. V první rovině jde o zvýšení ochrany majetkových práv tím, že dojde k doplnění § 207 TZK o základní skutkovou podstatu, jejíž znění by mohlo být následovné: „***Kdo bez souhlasu oprávněné osoby užije počítačový systém.“***

Tímto ustanovením by byla vymezena i okolnost, která spočívá v zásahu do majetkového práva jiného. V případě neoprávněného užívání cizí věci ve vztahu k počítačovému systému není řešením snížení škody z nikoli malé na nikoli nepatrnou (viz § 207 odst. 1 al. 1 TZK), neboť cena řady počítačových systémů je v současnosti nižší i než hodnota nikoli nepatrná (tedy nejméně 5000,- Kč), a přesto jsou tyto počítačové systémy schopny zcela plnit zadanou činnost v rámci sítě botnet.

Druhá rovina, která vystihuje závažnost jednání útočníka, pak spočívá ve včlenění nové kvalifikační okolnosti do § 230 odst. 3 TZK, přičemž tato okolnost by mohla znít následovně:

„úmyslně připojí počítačový systém do počítačové sítě s úmyslem spáchat trestný čin, či jej v této síti se stejným úmyslem užije,“

---

[1] **Bot** (zkrácenina ze slova robot). Jedná se o program, který umí plnit příkazy útočníka, zadávané z jiného počítačového systému. Nejčastěji se jedná o infikaci počítače virem typu worm, trojský kůň aj. Počítačový systém, který je takto na dálku ovládán, je pak označován jako **zombie**. Některé zdroje však i infikovaný počítačový systém označují jako bot.

Bot může vykonávat sběr dat, zpracovávat požadavky, rozesílat zprávy, komunikovat s řídícím prvkem aj.

[2] Blíže viz *Distribuované výpočty.* [online]. [cit.2.11.2013]. Dostupné z: http://dc.czechnationalteam.cz/

[3] Blíže viz PLOHMANN, Daniel, Elmar GERHARDS-PADILLA a Felix LEDER. *Botnets: Detection, Measurement, Disinfection & Defence.* ENISA, 2011. [online]. [cit.17.5.2015], s. 14. Dostupné z: https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence

Další definice botnetu a informace o nich je možné nalézt např. na:

Co je to botnet a jak se šíří? [online]. [cit.15.7.2016]. Dostupné z:

Botnety: nová internetová hrozba. [online]. [cit.15.7.2016]. Dostupné z: http://www.lupa.cz/clanky/botnety-internetova-hrozba/

Války síťových robotů– jak fungují sítě botnets. [online]. [cit.15.7.2016]. Dostupné z: http://tmp.testnet-8.net/docs/h9_botnet.pdf

Botnets. [online]. [cit.15.7.2016]. Dostupné z: https://www.youtube.com/watch?v=-8FUstzPixU&index=2&list=PLz4vMsOKdWVHb06dLjXS9B9Z-yFbzUWI6

[4] Obrázek centralizovaného botnetu. Blíže viz PLOHMANN, Daniel, Elmar GERHARDS-PADILLA a Felix LEDER. *Botnets: Detection, Measurement, Disinfection & Defence.* ENISA, 2011. [online]. [cit.17.5.2015], s. 16. Dostupné z: https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence

[5] Obrázek decentralizovaného botnetu. Tamtéž s. 18

[6] Malware economy. Blíže viz PLOHMANN, Daniel, Elmar GERHARDS-PADILLA a Felix LEDER. *Botnets: Detection, Measurement, Disinfection & Defence.* ENISA, 2011. [online]. [cit.17.5.2015], s. 21. Dostupné z: https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence

[7] *Bots and Botnets – A growing Threat.* [online]. [cit.11.8.2016]. Dostupné z: https://us.norton.com/botnet/

[8] Tabulka vznikla na základě spojení informací z následujících zdrojů:

Botnet. [online]. [cit.15.7.2016]. Dostupné z: https://en.wikipedia.org/wiki/Botnet

Botnet – Historical List of Botnets. [online]. [cit.15.8.2016]. Dostupné z: http://www.liquisearch.com/botnet/historical_list_of_botnets

Botnet. [cit.8.7.2016]. Dostupné z: http://research.omicsgroup.org/index.php/Botnet

Historical list of botnets. [online]. [cit.15.8.2016]. Dostupné z: http://jpdias.me/botnet-lab//history/historical-list-of-botnets.html

[9] *Fridge caught sending spam emails in botnet attack.* [online]. [cit.17.5.2016]. Dostupné z: http://www.cnet.com/news/fridge-caught-sending-spam-emails-in-botnet-attack/

[10] Blíže viz NIGAM, Ruchna. *A timeline of Mobile Botnets.* [online]. [cit.12.7.2016]. Dostupné z: https://www.botconf.eu/wp-content/uploads/2014/12/2014-2.2-A-Timeline-of-Mobile-Botnets-PAPER.pdf

[11] Toto ustanovení počítá se způsobením škody na cizím majetku, přičemž škoda musí být nikoli malá (tj. minimálně 25 000,- Kč viz § 138 odst. 1 TZK).

4.3. Malware

Za **malware** (složenina anglických slov malicious software – škodlivý software), je možné označit jakýkoli software využitý k narušení standardní činnosti počítačového systému, zisku informací (dat), či využitý k získání přístupu k počítačovému systému. Malware může mít celou řadu podob, přičemž mnohé druhy malware jsou pojmenovány podle toho, jakou činnost provádějí.

Jeden malware je schopen plnit několik funkcí (vykonávat několik činností) naráz. Může se například sám dále šířit prostřednictvím e-mailů (v rámci přílohy) nebo jako data v P2P sítích a zároveň může získávat například e-mailové adresy z napadeného počítačového systému.

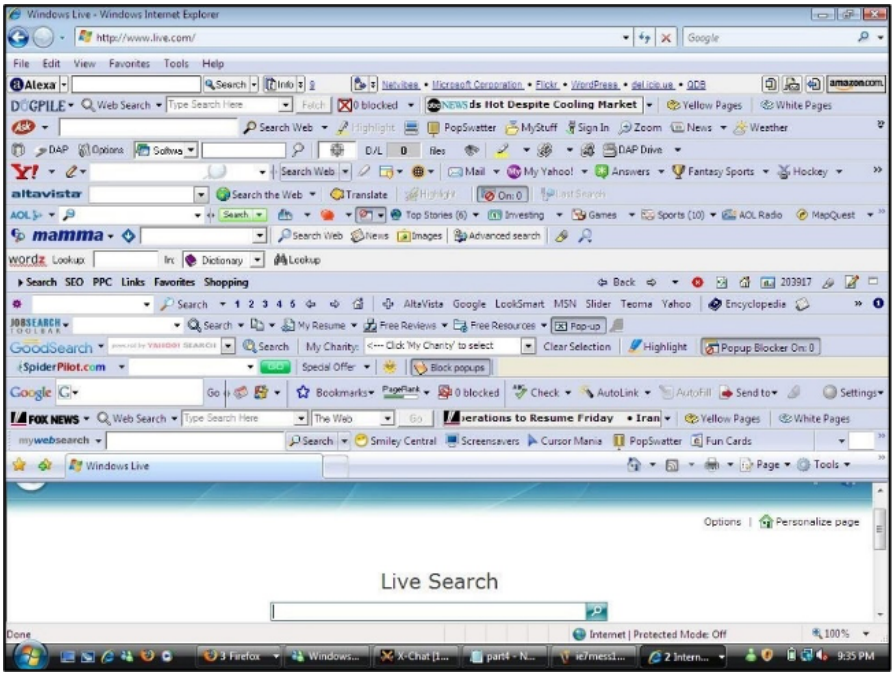
Z historického hlediska existovala nejdříve řada různých termínů pro software, který je v současnosti označován souborným pojmem malware. Vlastní názvy konkrétního škodlivého software vznikaly zpravidla podle činnosti, kterou daný program vykonával. I přes právě uvedené konstatování, že je v současnosti využíván primárně pojem malware, je stále možné se setkat i s historicky starším označením škodlivého software. Jedná se o následující skupiny:

1. **Adware**
2. **Spyware**
3. **Viry (Viruses)**
4. **Červi (Worms)**
5. **Trojské koně (Trojan Horses)**
6. **Backdoor**
7. **Rootkity**
8. **Keylogger**
9. **Ransomware aj.**[1]

Ad 1) Adware

Pojem adware je zkratka z anglického slovního spojení „*advertising supported software*", což lze do českého jazyka volně přeložit jako software podporující reklamu. Jedná se o nejméně nebezpečnou, avšak výnosnou formu malware.[2] Adware zobrazuje reklamy na počítačovém systému uživatele (např. pop-up okna v operačním systému[3] nebo na webových stránkách, reklamy zobrazované společně se software aj.). Byť jde ve většině případů o produkty, které pouze obtěžují uživatele neustálými reklamními sděleními, která „vyskakují" na obrazovce, může být adware spojen i se spyware, jehož účelem je sledovat činnost uživatele a odcizit důležité informace.

Adware



Ukázka Adware a dalších add on nainstalovaných ve webovém prohlížeči [4]

Ad 2) Spyware

Pojem spyware je složeninou anglických slov „*spy*" (špion) a „*software*". Pomocí spyware jsou získávána statistická data[5] o provozu počítačového systému a bez vědomí a souhlasu uživatele odesílána do datové schránky útočníka. Součástí těchto dat mohou být i informace osobního charakteru či informace o osobě uživatele, dále informace o navštívených webových stránkách, o spuštěných aplikacích apod.

Spyware může být jednak instalován jako samostatný malware, jakož může být často i součástí jiných, volně šířených a jinak zcela bezpečných programů. V takovém případě je instalace a další činnost spyware typicky ošetřena ve smluvních podmínkách EULA a uživatel tak zpravidla nevědomky dobrovolně souhlasí s monitorováním vlastních aktivit. Přikládání spyware programů k programům jiným (např. klientské programy P2P sítě, různé shareware programy aj.) bývá motivováno snahou výrobce programu zjistit zájmy či potřeby uživatele a tyto informace využít např. pro cílenou reklamu.[6] Charakteristickou vlastností programů typu spyware, která jsou součástí „balíčku programů", je též fakt, že většinou zůstávají nainstalovány v počítači i poté, co hlavní program byl odinstalován, což ve většině případů bývá uživateli skryto.

Spyware představuje hrozbu jednak proto, že odesílá různé informace z počítačového systému uživatele k „útočníkovi" (přičemž tyto informace jsou dále zpracovávány a dochází ke korelaci dat s daty a informacemi získanými z jiných zdrojů), a jednak pak proto, že spyware může obsahovat další nástroje, které ovlivňují vlastní činnost uživatele[7].

Ad 3) Viry (Viruses)

Jedná se o program či závadný kód, který sám sebe připojí k jinému existujícímu spustitelnému souboru (např. software aj.) či dokumentu. Virus se reprodukuje v momentě, kdy dojde ke spuštění tohoto software či otevření infikovaného dokumentu. Nejčastěji se viry šíří díky sdílení software mezi jednotlivými počítačovými systémy; ke svému šíření nepotřebují součinnost uživatele. Viry byly dominantní formou malware zejména v 80. a 90. letech 20. století.[8]

Existuje velká řada virů, jejichž účelem je ničit, jiné naopak mají za úkol „usídlit" se v co největším počtu počítačových systémů a tyto pak využít k cílenému útoku. Typické pro tyto programy je schopnost šířit se mezi systémy bez nutnosti zásahu uživatele počítačového systému. Projevy virů mohou být různé, např. od neškodného vyhrávání melodie, přes zahlcení systému, změnu či zničení dat, až po celkovou destrukci napadeného systému. Počítačové viry je možno třídit podle mnoha různých hledisek, např. podle hostitele (tedy podle druhu programů, které počítačové viry přenášejí), podle způsobů, kterým se projevují v systému, podle umístění do paměti atd.[9] Podle toho, jaké soubory viry napadají, je možné je rozdělit na:

§ boot viry (napadají pouze systémové oblasti)

§ souborové viry (napadají pouze soubory)

§ multiparitní viry (napadají soubory i systémové oblasti)

§ makroviry (napadají aplikace pomocí maker)

Ad 4) Červi (Worms)

Za viry bývají označováni i tzv. **počítačoví červi** (anglicky „*worm*"). Důvodem bližší spojitosti s viry je ta skutečnost, že červi nepotřebují žádného hostitele, tedy žádný spustitelný soubor (obdobně jako viry). Tyto programy se na rozdíl od virů, které bývají připojeny jako součást jiného programu, šíří zpravidla samostatně. Napadený systém je následně červem využit k dalšímu odeslání kopií sebe sama dalším uživatelům pomocí síťové komunikace.[10] Tímto způsobem se velmi rychle rozšiřuje, což může vést až k zahlcení počítačové sítě, a tím i celé infrastruktury. Na rozdíl od virů jsou tyto programy schopny analyzovat bezpečnostní slabiny v zabezpečení napadeného informačního systému,[11] proto bývají taktéž využívány k vyhledávání bezpečnostních mezer v systémech nebo v poštovních programech.[12]

Ad 5, 6) Trojské koně (Trojan Horses) a Backdoors

Za **trojské koně** jsou obecně označovány ty počítačové programy, které obsahují skryté funkce, s jejichž užitím uživatel nesouhlasí nebo o nich neví, a které jsou potenciálně nebezpečné pro další fungování systému. Stejně jako v případě virů mohou být tyto programy připojeny k jinému, bezpečnému programu či aplikaci nebo mohou samy vypadat jako neškodný počítačový program. Trojské koně, na rozdíl od klasických virů, nejsou schopny se replikovat a ani se šířit bez „pomoci" uživatele. V případě, že je trojský kůň aktivován, může být využit například k mazání, blokování, modifikaci, kopírování dat či například narušování běhu počítačového systému, či počítačových sítí.

Některé trojské koně po své aktivaci bez vědomí uživatele otevírají komunikační porty počítače, čímž výrazným způsobem zjednodušují další napadání takto zasaženého systému jinými škodlivými programy, popřípadě usnadňují přímé ovládnutí napadeného počítače tzv. na dálku. Takové trojské koně jsou označovány jako **backdoor** (z anglického „*backdoor*" - zadní vrátka).[13] Moderní backdoor programy mají zdokonalenou komunikaci a využívají většinou protokolů některých nástrojů komunikace, jako je např. program ICQ.[14]

S užitím trojských koní bývá často též spojeno užití různých **skenovacích** (či scanovacích)[15] **programů** (angl. „*port scannery*"), což jsou programy, které slouží zejména ke zjištění, které komunikační síťové porty počítače jsou otevřené, jaké služby jsou na nich spuštěné a zda je přes ně možno realizovat útok na takový systém. Tato data jsou opět zasílána útočníkovi a jsou dále potenciálně využitelná při páchání dalších kybernetických útoků.

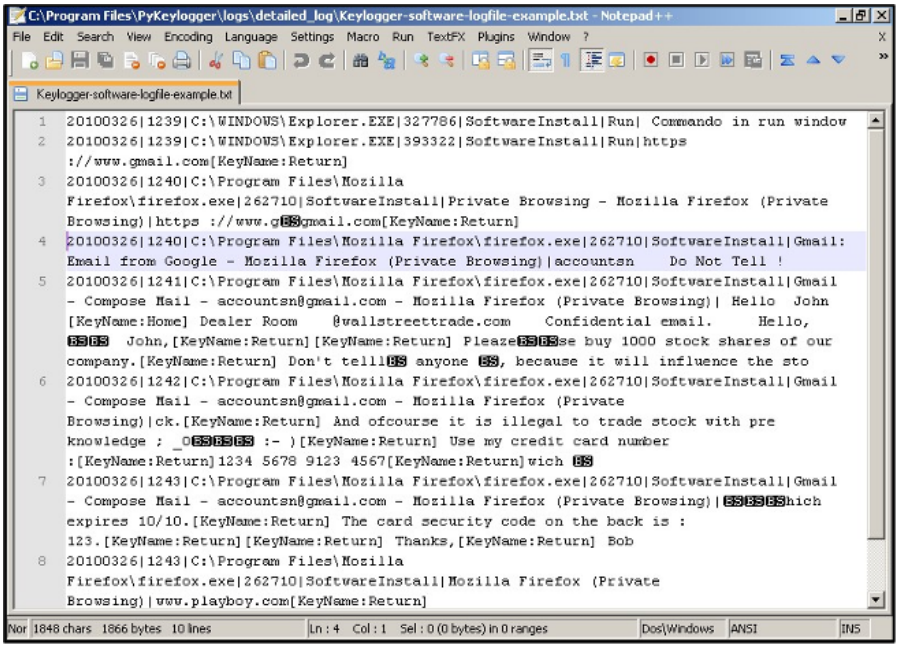
Ad 7) Rootkity

Tímto pojmem jsou označovány nejen počítačové programy, ale i celá technologie sloužící k zamaskování přítomnosti malware (např. počítačových virů či trojských koní, červů aj.) v napadeném systému. Nejčastěji mají formu nepříliš objemných počítačových programů. Rootkity nejsou škodlivé samy o osobě, ale jsou využívány právě tvůrci škodlivých programů, jako jsou např. viry, spyware atd.[16] Program typu rootkit mění chování celého operačního systému, jeho částí nebo nadstavbových aplikací tak, aby se uživatel o existenci nebezpečných programů ve svém počítačovém systému nedozvěděl. Obecně lze programy typu rootkit rozdělovat na **systémové** (modifikující jádro systému) a **aplikační** (modifikují konfiguraci aplikací).[17]

Z aplikací napadají rootkity zejména specializované programy na vyhledávání a odstraňovaní nebezpečných programů ze systému, tedy antiviry apod. [18] Antivirové programy při použití rootkit programu nemohou tento škodlivý program z napadeného systému odstranit. Tímto způsobem je přítomnost škodlivého programu v napadeném systému prodlužována. Z tohoto hlediska je možno konstatovat, že programy typu rootkit mohou být velmi snadno zneužitelné při páchání trestné činnosti spojené s užitím či zneužitím informačních technologií.[19] Některá literatura označuje tyto nástroje jako podskupinu backdoor trojských koní.[20]

Ad 8) Keylogger (Keystroke Logger)

Keylogger je software zaznamenávající konkrétní stisky kláves na napadeném počítačovém systému. Nejčastěji je keylogger využíván k zaznamenání přihlašovacích údajů (uživatelského jména a hesla) k účtům, k nimž je z počítačového systému přistupováno. Získané informace pak jsou typicky zaslány útočníkovi.



Ukázka činnosti keyloggeru[21]

Ad 9) Ransomware

Ransomware bude detailněji popsán v samostatné kapitole.

Distribuce malware

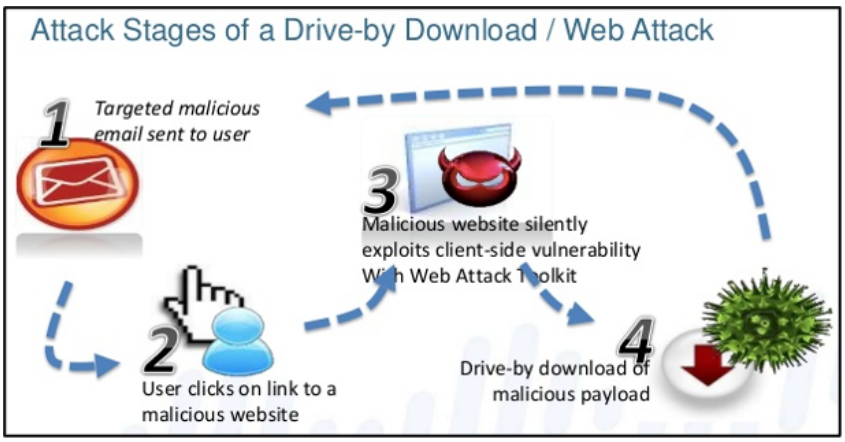
Existuje celá řada způsobů, jimiž je možné malware doručit k cílovému počítačovému systému. Na tomto místě stručně uvedu některé metody šíření malware. Malware je možné distribuovat skrze:

§ **Přenosná paměťová média**

Například pomocí CD, DVD, USB, externí disk aj. Jedná se o nejstarší, avšak stále účinný způsob distribuce malware, kdy si uživatelé navzájem předávají infikované soubory **či počítačové sítě** obsahující **infikované soubory** (sdílení takovýchto souborů v rámci počítačových sítí, typicky P2P sítí).

§ **Drive-by-download**

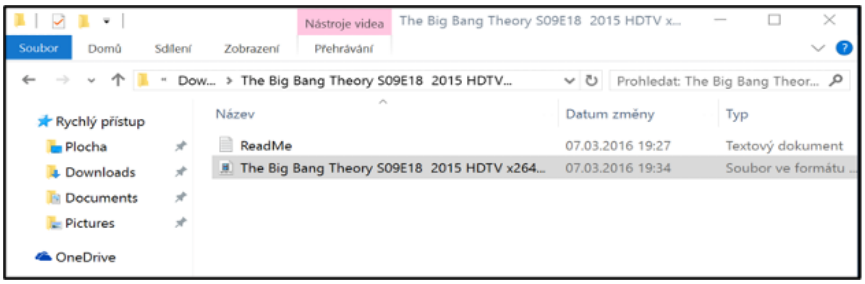
Jedním z nejčastějších způsobů infekce malware je jeho stažení z Internetu a následné spuštění souboru, typicky s příponou .exe (executable file – spustitelný program) z neznámého zdroje. Může se jednat o falešné či padělané programy (např. napodobeniny Flapp Bird, falešné media kodeky aj.), programy sloužící k obcházení ochrany autorských práv (cracky, keygeny aj.), reálné infikované programy aj.

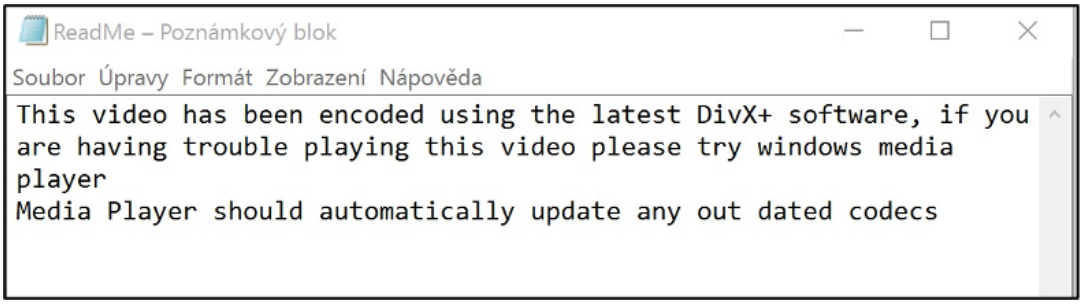


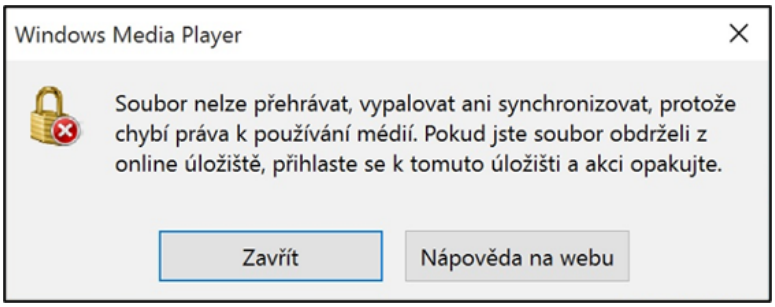
Obrázek 39 - Zobrazení jednoho z možných principů drive by download. [22]

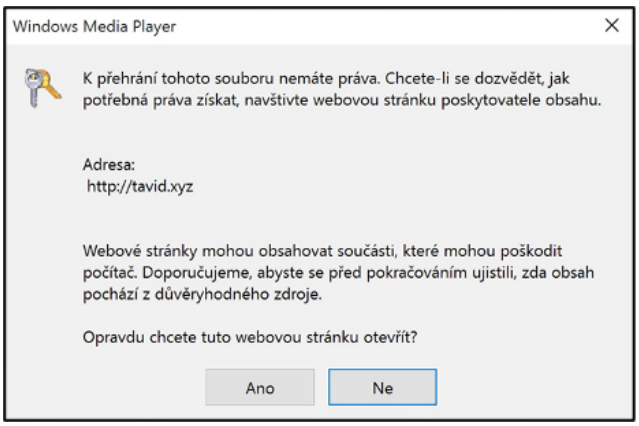
Následující příklad ukazuje malware stažený uživatelem skrze P2P síť (konkrétně se jednalo o soubor s dílem seriálu *The Big Bang Theory – sezona 9, díl 18*). Tento malware vyzval uživatele ke stažení nového kodeku přes Media player, aby mohlo být video přehráno. Media player se začal připojovat na stránky útočníka a následně došlo k fiktivní instalaci kodeku, avšak ve skutečnosti byl do počítače nainstalován malware (v tomto případě se jednalo o kombinaci malware: backdoor, keylogger, bot), který umožnil útočníkovi zcela ovládnout počítačový systém uživatele.

V tomto případě byla zarážející i ta skutečnost, že nabízený díl *The Big Bang Theory* ještě nebyl odvysílán v USA, kde má premiéru, přesto měl počet stažení v řádech desítek tisíc.









- **„Kancelářské dokumenty“**

Velmi často dochází k šíření malware v těle souborů například typu: .doc, . xls, .avi aj. Tímto způsobem je možné distribuovat pouze makroviry. Uživatel předpokládá, že otevírá wordový dokument, avšak zároveň spouští executable file, který se jako tento dokument maskuje.

- **e-mail**

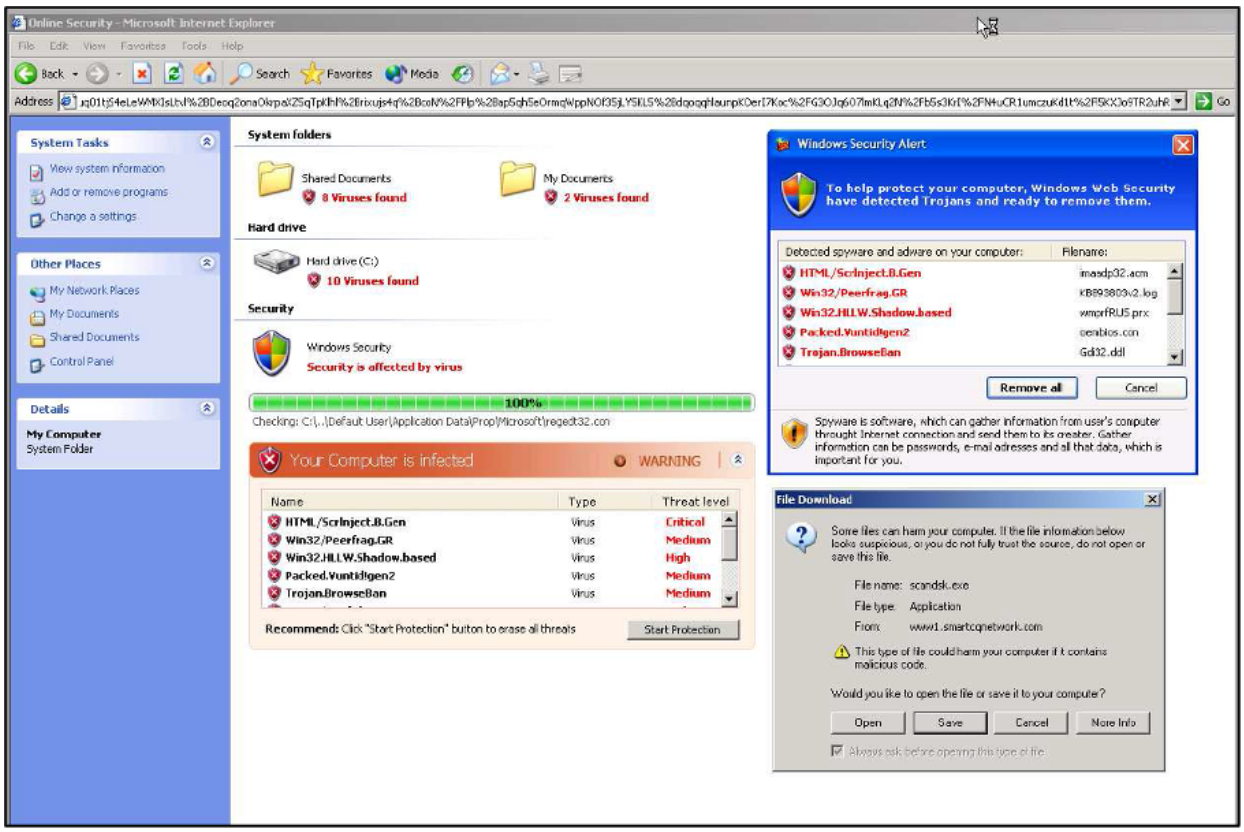
Malware může být uložen v příloze zprávy, nebo se může jednat o skripty uvnitř HTML[23] těla e-mailů. V současnosti se jedná o jeden z nejběžnějších způsobů distribuce malware. Jako příklad je možné uvést současné phishingové kampaně, hoax, spam aj.

- **HTML**

Malware může být umístěn přímo na webových stránkách, nebo v jednotlivých skriptech.

- **Falešný antivirus**

Uživateli je typicky nabídnut antivirus zdarma – jako adware. Tento antivirus provede „otestování počítače“ a objeví závažné zranitelnosti a malware, jež uživatelův antivirus nedetekoval. Falešný antivirus kombinuje útok sociálním inženýrstvím (vzbuzení obavy před škodlivým software) s instalací malware obsaženým právě ve falešném antiviru.



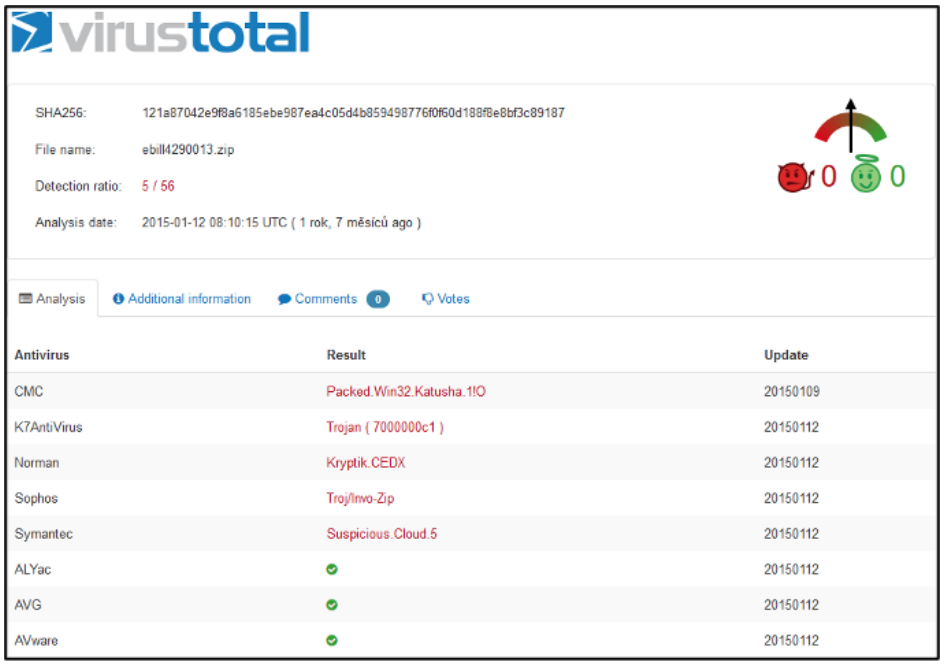
Falešný antivirus

Falešný antivirus[24]

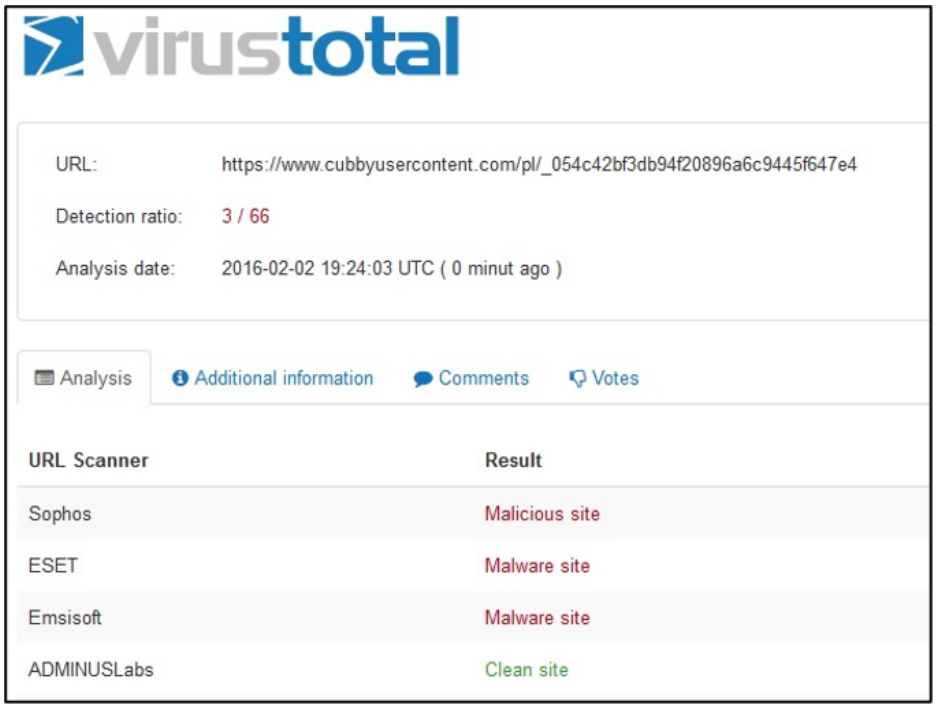
Pokud si uživatel není jistý, zda soubor či webová stránka obsahuje malware, může využít celou řadu nástrojů, které mu pomohou ověřit si přítomnost škodlivého software.

Jednou z osvědčených služeb je služba **https://www.virustotal.com/** . Na této stránce může uživatel zadat oskenování souboru až do velikosti 128 MB či si může nechat prověřit webovou stánku, na kterou hodlá vstoupit (vhodné je tento sken provádět např. při návštěvě stránek s internetovým bankovnictvím či stránek, na nichž je prováděna platba. Pro ověření je třeba překopírovat **celé URL navštívené stránky**.). Služba Virustotal propojuje společnosti zabývající se kybernertickou bezpečností, vývojem antivirových prostředků atp., přičemž uživatelův požadavek je prověřen nástroji všech těchto společností, čímž se zvyšuje pravděpodobnost odhalení škodlivého software.

Následující printscreen zobrazuje výsledek prověření nově doručeného souboru v rámci phishingové kampaně. Den po začátku této kampaně identifikovalo malware v přiloženém souboru pouze 5 společností, do týdne jej byly schopny identifikovat i všechny ostatní společnosti. Nicméně právě doba mezi doručením aktualizací do antivirů uživatelů na jejich počítačových systémech a začátkem útoku je pro případný úspěch útočníka rozhodující.



Výsledek testování souboru



Výsledek testování webové stránky

Malware je možné nainstalovat téměř do jakéhokoli počítačového systému. Jako příklady specifických instalací mohou sloužit případy instalace **micromalware.** Jedná se o škodlivý kód, který je rozšiřován na poměrně malém počtu počítačových systémů. Tento kód vykazuje abnormální chování a bezpečnostní programy na něj často nedokážou reagovat. Nejznámějším případem micromalware je **červ STUXNET**.[25], či instalace botnet klienta do již zmíněné lednice.

Samostatnou kapitolu pak představuje malware určený pro mobilní zařízení (**mobile malware**). První malware navržený k útokům na mobilní telefony byl objeven přibližně v roce 2004. Dnes Kaspersky Lab, která o tomto objevu tehdy informovala, uvádí, že existuje více než **340 000 malwarů.**[26]

Pokud bychom se zaměřili na nejohroženější operační systém v rámci mobilních zařízení, pak nejvíce hrozeb je cíleno na OS Android. Důvodem této skutečnosti je především rozmanitost používaných verzí operačního systému a jejich neaktuálnost. **Většina zařízení s OS Android neumožňuje aktualizovat operační systém na poslední verzi, která je zpravidla upravena tak, aby odolávala známým zranitelnostem a již má opraveny chyby z předchozích verzí tohoto operačního systému.** [27] **Přitom je odhadováno, že 77 % hrozeb útočících na OS Android by bylo možné eliminovat právě používáním nejnovější verze tohoto operačního systému.**

Útočníci v případě mobilních zařízení využívají především:

- **Neaktuální verze operačního systému mobilního zařízení** (známé zranitelnosti jednotlivých systémů);

- **Minimální zabezpečení mobilního zařízení** antivirovým prostředkem;

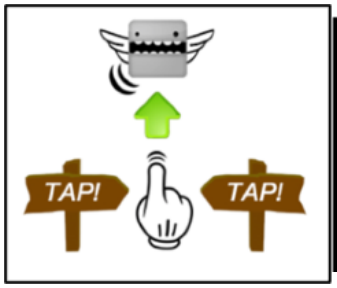
- **Neznalosti uživatelů** (Řada uživatelů bez rozmyslu instaluje aplikace „z neznámého zdroje" či aplikace požadující nadměrný přístup a oprávnění v rámci zařízení.);

- **Sociální inženýrství a „vlny zájmu" o aplikace určitého typu.**

Jedním z důvodů, proč je jako primární operační systém napadán systém Android, je i ta skutečnost, že v rámci distribučního kanálu (Google Play) není ověřována bezpečnost aplikací (respektive to, zda konkrétní aplikace například neobsahuje malware), jako tomu například je u operačního systému iOS a jejich distribučního kanálu (App Store).

Jako příklad výše uvedeného je možné uvést aplikaci **Flappy Bird** a její „klony". Tuto aplikaci vyvinul Nguyễn Hà Đông a do distribuce pro iOS byla uvedena 24. května 2013. Pro Android OS začala být tato aplikace dostupná v roce 2014 a v lednu 2014 se stala nejstahovanější hrou zdarma. Tvůrce hru z trhu odstranil 10. února 2014. Hra zaznamenala více jak 50 milionů stažení.

Již v době, kdy byla originální hra Flappy Bird na trhu, se začaly objevovat různé klony této hry pro OS Android, z nichž řada profitovala pouze na úspěchu originálu. Do řady dalších verzí však byl záměrně umístěn malware, přičemž je odhadováno, že až 79 % klonů této hry bylo infikováno škodlivým software.[28] Mezi infikované klony patří například tyto produkty:



Infikování mobilního telefonu může být jedním z primárních cílů útočníka, neboť tato zařízení se dnes typicky používají v rámci dvoufaktorové autentizace internetového bankovnictví či nakupování. Útočníci se snaží získané informace použít například k odčerpání finančních prostředků přímým přístupem do bankovního účtu uživatele prostřednictvím služby internet banking nebo získání citlivých informací.

Možnosti trestněprávního postihu v ČR

V ČR je možné postihnout útok pomocí malware dle **§ 230** (Neoprávněný přístup k počítačovému systému a nosiči informací) TZK. **Držení malware, s úmyslem spáchat trestný čin** dle § 182 (Porušení tajemství dopravovaných zpráv) či trestný čin dle § 230 TZK**, je trestné dle § 231** (Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat) TZK. Pokud by **účelem viru** bylo získat například utajované skutečnosti, či podpora teroristické skupiny, mohl by se útočník například dopustit trestných činů **§ 311** (Teroristický útok), **§ 316** (Vyzvědačství) nebo **§ 317** (Ohrožení utajované informace) **ve stádiu přípravy** TZK.

---

[1] Nejedná se o kompletní výčet různých typů malware. Spíše jde o vymezení základních typů malware včetně vysvětlení jejich fungování.

[2] Existují společnosti specializující se na „placení za instalaci" (*PPI, pay per install*). *„PPI se pak projevuje záplavou aktivit vedoucích k instalaci add-onů či dalšího nechtěného softwaru, který (v tom nejméně škodlivém případě) bez vědomí uživatelů vyměňuje reklamy ve webových stránkách, případně je vkládá tam, kde žádné reklamy na webu nejsou....**Celý model PPI je postaven na tom, že ti, kdo tyto služby nabízejí, neberou žádné ohledy na to, jestli uživatel něco chce instalovat. Za každou instalaci dostávají až 1,50 USD**, je tedy více než jisté, že podvodné a automatické instalace jsou zásadním prvkem jejich „obchodního modelu."*

Blíže viz DOČEKAL, Daniel. *Google: Adware napadá miliony zařízení a poškozuje inzerenty, weby i uživatele.* [online]. [cit.10.8.2016]. Dostupné z: http://www.lupa.cz/clanky/google-adware-napada-miliony-zarizeni-a-poskozuje-inzerenty-weby-i-uzivatele/

[3] Obrázek těchto pop-up oken. Blíže viz *Adware.* [online]. [cit.10.8.2016]. Dostupné z: http://www.mhsaoit.com/computer-networking-previous-assignments/324-lesson-16-h-the-secret-history-of-hacking

[4] [online]. [cit.10.8.2016]. Dostupné z: https://i.ytimg.com/vi/GcvIB-EpMwA/maxresdefault.jpg

[5] Např. přehled navštívených webových stránek, jejich IP adresy, přehledy nainstalovaných a užívaných programů, záznamy o downloadu souborů z Internetu, údaje o struktuře a obsahu adresářů uložených na pevném disku atd.

[6] [cit.8.1.2008]. Dostupné z: http://www.spyware.cz/go.php?p=spyware&t=clanek&id=9

[7] Může se jednat např. o: **Browser Helper Object** (DLL knihovna, umožňující programátorům změnit a sledovat Internet Explorer); **Hijacker** (software měnící domácí stránku webového prohlížeče); **Dialery** [přesměrovává telefonní linku na drahé telefonní tarify (v současnosti hlavně útoky na mobilní telefony a VoIP ústředny)]; **Keystroke Logger/Keylogger** (monitoring stlačených kláves); **Remote Administration** (umožní vzdálenému uživateli, ovládat počítačový systém uživatele na dálku); **Tracer** (program, sledující pohyb počítačového systému – typicky mobilního zařízení) aj.

[8] Blíže viz Muzeum malware. *The Malware Museum @ Internet Archive*. [online]. [cit.17.5.2016]. Dostupné z: https://labsblog.f-secure.com/2016/02/05/the-malware-museum-internet-archive/

[9] Blíže např. POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Aleš Čeněk, 2005, s. 216 a násl.

[10] Blíže např. LI, Tao, GUAN, Zhihong, WU, Xianyong. Modeling and Analyzing the Spread of Active Worms Based on P2P Systems. *Computers & Security*, 2007, roč. 26, č. 3, s. 213 – 218.

[11] Blíže srov. RAK, Roman a Radek KUMMER. Informační hrozby v letech 2007 – 2017. *Security magazín*, 2007, roč. 14, č. 1, s. 4.

[12] Srov. JIROVSKÝ, Václav a Oldřich KRULÍK. Základní definice vztahující se k tématu. *Security magazín*, 2007, roč. 14, č. 2, s. 47.

[13] Přehled nejrozšířenějších trojských koní spolu s výpisem jejich funkcí a komunikačních portů je možno získat na různých webových stránkách dostupných na Internetu. Blíže srov. např. http://www.test.bezpecnosti.cz/full.php

[14] Srov. JIROVSKÝ, Václav. K*ybernetická kriminalita. Nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, s. 63.

[15] Tyto programy jsou označovány někdy též jako skanovací, skanerovací, skenerové či skenovací programy.

[16] Blíže srov. např. BALIGA, Arati, Liviu IFTODE a Xiaoxin CHEN. Automated Containment of Rootkits Attacks. *Computers & Security*, 2008, roč. 27, č. 7-8, s. 323 – 334.

BAUDIŠ, Pavel. Programy typu rootkit. Další hrozba pro Windows. *CHIP*, 2005, č. 7, s. 14

[17] Srov. RAK, Roman a Radek KUMMER. Informační hrozby v letech 2007 – 2017. *Security magazín*, 2007, roč. 14, č. 1, s. 5.

[18] Např. trojský kůň DNS-Changer napadá nejprve bezpečnostní programy, kde sám sebe odstraní ze seznamu škodlivých programů, čímž znemožní svoje objevení. Blíže. PLETZER, Valentin. Demaskovaný spyware. *CHIP*, 2007, č. 10, s. 116 – 120.

[19] Blíže k této problematice např. PŘIBYL, Tomáš. Seznamte se s rootkity. *PC World*, 2007, č. 9, s. 108 – 110.

[20] JIROVSKÝ, Václav. *Kybernetická kriminalita. Nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, s. 65

[21] Zachytávání klávesových stisků a informací o spuštěných souborech. [online]. [cit.10.8.2016]. Dostupné z: http://img.zerosecurity.org/files/2013/10/Keylogger-software-logfile-example.jpg

[22] [online]. [cit.10.7.2016]. Dostupné z: https://image.slidesharecdn.com/delljointevent2014november-onur-141105074412-conversion-gate02/95/end-to-end-security-with-palo-alto-networks-onur-kasap-engineer-palo-alto-networks-23-638.jpg?cb=1415174438

[23] Hyper Text Markup Language – jde o název značkovacího jazyka používaného pro tvorbu webových stránek.

[24] Dvě verze falešného antiviru. [online]. [cit.10.8.2016]. Dostupné z: http://www.cctslo.com/images/fake-personal-antivirus.jpg

[25] Blíže viz např. *Stuxnet.* [online]. [cit.23.7.2016]. Dostupné z:https://cs.wikipedia.org/wiki/Stuxnet

[26] Blíže viz *The very first mobile malware: how Kaspersky Lab discovered Cabir*. [online]. [cit.29.6.2015]. Dostupné z: http://www.kaspersky.com/about/news/virus/2014/The-very-first-mobile-malware-how-Kaspersky-Lab-discovered-Cabir

Dále viz např.:

Škodlivý kód cílí na mobily, šíří se jako lavina. [online]. [cit.17.5.2016]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/401956-skodlivy-kod-cili-na-mobily-siri-se-jako-lavina.html

Warning! Over 900 Milion Android Phones Vulnerable to New „QuadRooter" Attack. [online]. [cit.10.8.2016]. Dostupné z: https://thehackernews.com/2016/08/hack-android-phone.html

[27] Dle statistik je u OS Android následující procentuální zastoupení všech zařízení s tímto OS: Marshmallow 6.0 – 7,5 %; Lollipop 5.1 – 19,4 %; Lollipop 5.0 – 16,2%; KitKat 4.4 – 32,5%; Jelly Bean 4.1,2,3 – 20,1%; starší verzi – 4,3%.

Blíže viz např. *Android version market share distribution among smartphone owners as of May 2016.* [online]. [cit.14.8.2016]. Dostupné z: http://www.statista.com/statistics/271774/share-of-android-platforms-on-mobile-devices-with-android-os/

[28] Blíže viz např. *Flappy Bird Clones Help Mobile Malware Rates Soar.* [online]. [cit.14.8.2016]. Dostupné z: http://www.mcafee.com/us/security-awareness/articles/flappy-bird-clones.aspx

4.4. Ransomware

Do skupiny malware se řadí i tzv. vyděračský malware, pro nějž se ustálilo označení **ransomware**[1] (z anglického „*ransom*“ – výkupné, někdy také označovaný jako rogueware nebo scareware). Ransomware je malware, který brání či omezuje uživatele v řádném užívání počítačového systému do doby, než dostane útočník zaplaceno „výkupné“. Ransomware se nejčastěji dostane do počítače pomocí malware (trojského koně či červa), který je umístěn na webových stránkách, nebo je přílohou e-mailu. Jakmile je tento malware bezpečně „usídlen“ v počítačovém systému, dojde ke stažení vlastního ransomware.

Obecně je možné rozlišovat dva typy ransomware podle toho, jak moc zasahují do vlastního chodu počítačového systému. **Prvním typem je ransomware, který omezí funkčnost celého počítačového systému** a neumožní uživateli tento systém vůbec využívat (např. zabráněním spuštění operačního systému či zablokováním systémové obrazovky. Typickým příkladem tohoto typu je *„Policejní ransomware“* – viz dále). **Druhým typem pak je ransomware, jenž ponechá počítačový systém funkční, avšak dochází k uzamčení a znepřístupnění dat uživatele.**

V současnosti dochází spíše k využívání druhého typu ransomware, který je známý pod označením **crypto-ransomware.** Účelem tohoto malware je zašifrovat pevný disk nebo vybrané typy souborů v počítačovém systému, přičemž primárně má tento malware za cíl zašifrovat soukromé soubory uživatele jako jsou obrázky, textové či tabulkové dokumenty, videa aj. Po skončení šifrování se zpravidla uživateli zobrazí zpráva, že jeho soubory jsou zašifrovány, a pokud je chce získat zpět (dešifrovat), musí poslat určitý obnos na účet útočníka. Zpravidla jsou k transakcím využívány virtuální měny jako je Bitcoin nebo různé předplacené služby. Ve většině případů je stanovena časová lhůta pro zaplacení. Po uplynutí této lhůty dochází k smazání klíče, jenž může zašifrované soubory otevřít.

Evoluce ransomware

Ransomware, stejně jako každý jiný malware, prochází vývojem, přičemž první malware, který by bylo možné označit za ransomware, se objevil přibližně okolo roku 2005. Ve své podstatě se jednalo o **falešný antivirus (screware)**, který se za pomoci sociálního inženýrství snažil přesvědčit uživatele k zaplacení částky za vyčištění infikovaného počítačového systému. Tento ransomware zpravidla umožňoval uživateli využívat počítačový systém (nedošlo k jeho zamčení či zašifrování dat), avšak obtěžoval uživatele pop-up okny a upozorněními na neexistující viry v počítači. Tento ransomware byl velmi jednoduše odstranitelný.

Masivní nástup ransomware je možné datovat přibližně do roku 2011, kdy se celosvětově začal šířit ransomwarový útok blokující přístup k účtu uživatele OS Windows a oznamující, že počítač byl zablokován policií toho kterého státu.

Vlastní útok spočíval v tom, že se uživatel nakazil malware (typicky při návštěvě některých webových stránek[2] došlo k stažení „botnet-klienta“), a následně se stal součástí botnetu, přes který byl šířen vlastní „**policejní ransomware**“. Tento policejní ransomware následně zablokoval přístup k účtu uživatele[3] OS Windows s tím, že uživateli oznámil, že v jeho počítači byl nalezen materiál, který porušuje právo dané země (např. porušování práv autorských, dětská pornografie aj.). Zároveň byl uživatel „policií“ vyzván k zaplacení požadované sumy peněz, po níž dojde k odblokování počítače a „vyřešení celé věci“. V tomto případě útočníci využili techniky sociálního inženýrství, konkrétně obavy a důvěřivosti uživatele a pomocí odkazu na oficiální autority se od něj snažili získat finanční prostředky.

Zarážející na celém případu byla ta skutečnost, že značná část uživatelů ochotně zaplatila požadovanou částku (v ČR se tato částka průběžně pohybovala mezi 2000 - 4000 Kč), aniž by si ověřili, zda je skutečná policie oprávněna takovýmto způsobem blokovat počítače, či „vyřizovat“ případné prohřešky uživatele.

Následující printscreeny zobrazují „policejní ransomware“ v různých zemích a následně jsou zobrazeny verze použité v ČR.

Policejní ransomware[4]

Verze policejního ransomware určená pro Velkou Británii[5]

V Evropě se postupně objevovaly různé verze (rozuměj vzhled stránek) policejního ransomware. První verze byla zaznamenána na konci roku 2011, přičemž zobrazovala IP adresu připojení, ISP připojení a místo [kde byla uvedena IP adresa konkrétního poskytovatele (ISP) připojení], pokud měl uživatel zapnutou web kameru, došlo k vytvoření fotografie, která byla také zobrazena.

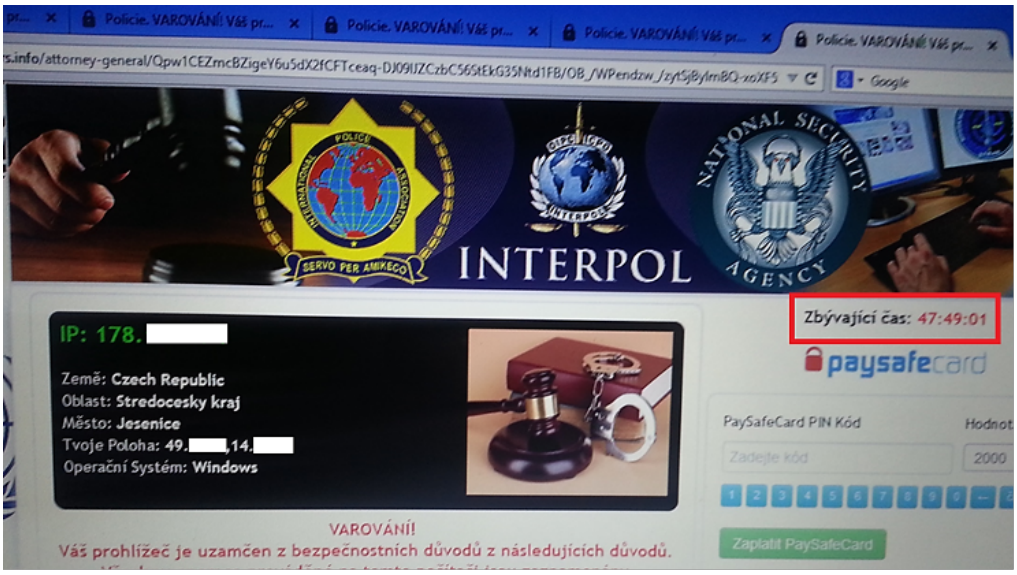
Policejní ransomware první verze v ČR

Novější verze, kromě toho, že se graficky lišily, navíc zobrazovaly verzi operačního systému a uživatelské jméno uživatele. Došlo také k vylepšení češtiny používané na zamknuté stránce.

Policejní ransomware ČR - další verze

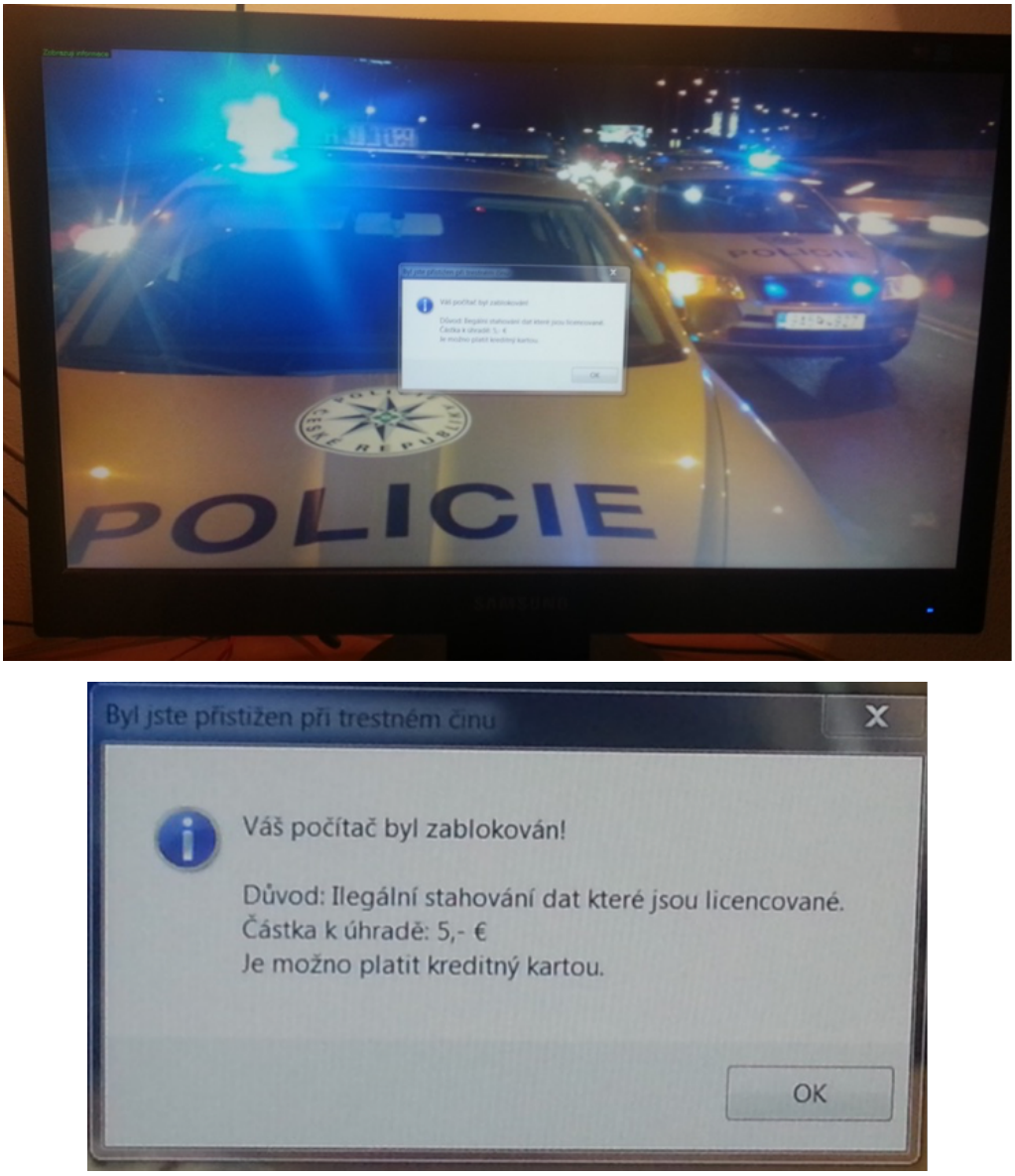
Výše popsaný „policejní ransomware" zažil největší rozmach v letech 2011 - 2013, nicméně další varianty tohoto škodlivého software se s různými obměnami objevily i později. Následující printscreeny zobrazují modifikace „policejního ransomware". Oba případy byly zjištěny v roce 2015. Na prvním printscreenu je zobrazen ransomware blokující dominantní webový prohlížeč využívaný v napadeném počítači (přičemž ostatní browsery infikovány nebyly). Uživatel mohl využívat všechny funkce počítačového systému, kromě napadeného prohlížeče.

Kromě dříve uvedených informací je zobrazena GPS pozice a zbývající čas do zaplacení.



Policejní ransomware ČR (r. 2015)

Druhý printscreen zobrazuje „zamknutý" počítač, přičemž ransomware byl skryt v cracku nelegálně stažené a nainstalované hry (v tomto případě se jednalo o hru Far Cry 4 staženou z českých torrentů).



Policejní ransomware ČR (r. 2015)

Od roku 2013 došlo v případě ransomware k významné změně. **Útočníci omezili útoky, které spočívaly v omezení funkčnosti celého počítačového systému, a primárně se zaměřili na zamykání dat uživatelů**. Zamykána jsou data na místních discích, discích připojených v rámci počítačové sítě i na všech připojených periferiích (např. externí USB, HDD aj.). Data se stávají „rukojmím", přičemž prolomení šifrování je téměř nemožné. Jedním z prvních ransomware tohoto typu byl CryptoLocker (dále pak CryptoWall aj.).

Cryptolocker (r. 2013)

Petya (r. 2017)

Mobile ransomware (r. 2018)

V rámci crime-as-a-service aktivit je nabízena od roku 2016 služba **Ransomware-as-a-service.** Uživatel (rozuměj útočník) má možnost si nadefinovat vlastní Ransomware dle svých představ. Zároveň mu je poskytnuto technické zázemí v podobě C&C serverů, bitcoinové peněženky, online 24/7 podpory aj. Příkladem Ransomware-as-a-service je software **Ransom32.**

Ransomware (klient)

Další změny je možné pozorovat i ve vlastní činnosti útočníků. Pokud dojde k instalaci ransomware, může být tento malware cílen například na šifrování uložených pozic ve hrách či může dojít k „zamknutí“ televize, které využívají operační systém Android.[6]

Prevenci a reakci na ransomware je možné shrnout do následujících bodů:

1. **Bezodkladně:**

· Zamezit propojování systémů navzájem mimo nezbytné případy

· Zamezit komunikaci do internetu vyjma nezbytných případů

- Změnit hesla privilegovaných účtů

2. **Do několika dnů:**

- Přesun záloh do offline, zkontrolovat funkčnost záloh
- Prověřit business continuity plány a přesunout je mimo systémy
- Nemazat data o kybernetických bezpečnostních incidentech
- Prověřit indikátory kompromitace
- Upozornit zaměstnance o riziku phishingu

3. **Do týdne:**

- Ověřit, že zálohy jsou odděleny tak, aby je ani privilegovaný administrátor nemohl smazat
- Zakázat použití nepodepsaných maker, pokud je to možné
- Zkontrolovat segmentaci sítě a řízení mezi segmenty
- Zpřísnit bezpečnostní politiky koncových stanic (zákaz spouštění neschválených aplikací, nepodepsaných PowerShell, ...)
- Pokud není business continuity management zaveden – zpracovat business continuity plány alespoň pro klíčové systémy
- Nasadit antiviry na všechna relevantní zařízení
- Zvážit aktualizaci otestovat ji a nasadit

4. **Dlouhodobá doporučení pro řešení ransomwarových útoků**

- Pravidelná školení zaměstnanců
- Výraznější segmentaci sítě
- Minimalizaci využívání administrátorských účtů
- Zálohovat, pravidelně testovat zálohy, držet zálohy offline
- Pravidlo 3 – 2 – 1 = Nejméně 3 kopie na 2 různých zařízeních, z toho 1 mimo organizaci.
- Mít plány kontinuity činnosti (BCM) a testovat je
- Pravidelně prověřovat aplikace přístupné ze sítě Internet a vyhodnocovat, zda jsou i nadále

Možnosti trestněprávního postihu v ČR

V ČR je možné postihnout útok pomocí malware, kterým je i ransomware, dle **§ 230** (Neoprávněný přístup k počítačovému systému a nosiči informací) TZK. **Držení malware, s úmyslem spáchat trestný čin** dle § 182 (Porušení tajemství dopravovaných zpráv) či trestný čin dle § 230 TZK**, je trestné dle § 231** (Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat) TZK.

V případě ransomware je možné uplatnit i ustanovení **§ 230 odst. 3** TZK, kdy útočník páchá tento trestný čin s úmyslem získat sobě nebo jinému neoprávněný prospěch. V úvahu by také mohlo přicházet uplatnění § 175 (Vydírání) TZK, kdy je osoba pohrůžkou jiné těžké újmy (např. i tím, že na ni bude podáno trestní oznámení[7]) nucena k zaplacení dané částky.

---

[1] Např. Reventon, CryptoLocker, CryptoWall, Loky, Petya, Cerber, SamSam, Jig Saw a další. Blíže viz např.:

Ransomware. [online]. [cit.14.8.2016]. Dostupné z: https://www.trendmicro.com/vinfo/us/security/definition/ransomware

Postřehy z bezpečnosti: Ransomware šestkrát jinak. [online]. [cit.14.8.2016]. Dostupné z: https://www.root.cz/clanky/postrehy-z-bezpecnosti-ransomware-sestkrat-jinak/

[2] Velmi často se jednalo o stránky s pornografií či jiným sexuálním materiálem. Na tyto stránky mohl být uživatel i přesměrován z jiné stránky, na níž byla „návnada".

[3] Aplikace byla nastavena jako „vždy navrchu" (StayOnTop). Uživatel nevidí jiné aplikace skryté pod tímto „ransom dialogem" a není schopen si vyvolat správce úloh. Vlastní Ransomware se zapsal do registrů Run a RunOnce a vždy po 500 ms prováděl kontrolu, ve stejném časovém rozsahu skrýval i správce úloh. Jedinou další běžící aplikací byla komunikace s C&C serverem (maskováno v procesu prohlížeče).

[4] *Policejní ransomware.* [online]. [cit.14.8.2016]. Dostupné z: https://www.f-secure.com/documents/996508/1018028/multiple_ransomware_warnings.gif/8d4c9ca2-fc77-433d-ac16-7661ace37f88?t=1409279719000

[5] [online]. [cit.14.8.2016]. Dostupné z: https://sophosnews.files.wordpress.com/2012/11/cool_ransom_uk_full.png

[6] Srov. např. *New Ransomware Encrypts Your Game Files.* [online]. [cit.14.8.2016]. Dostupné z: https://techcrunch.com/2015/03/24/new-ransomware-encrypts-your-game-files/

Android Ransomware now targerts your Smart TV, Too! [online]. [cit.14.8.2016]. Dostupné z: https://thehackernews.com/2016/06/smart-tv-ransomware.html

FLocker Mobile Ransomware Crosses to Smart TV. [online]. [cit.14.8.2016]. Dostupné z: http://blog.trendmicro.com/trendlabs-security-intelligence/flocker-ransomware-crosses-smart-tv/

[7] K pojmu jiná těžká újma viz ŠÁMAL, Pavel a kol. *Trestní zákoník II. § 140 až 421. Komentář.* 2. Vydání. Praha: C. H. Beck, 2012, s. 1752-1753

Konkrétně může *„pohrůžka jiné těžké újmy může spočívat v hrozbě způsobení majetkové újmy, vážné újmy na cti či dobré pověsti aj. Jinou těžkou újmou může být i zahájení trestního stíhání v důsledku oznámení trestného činu, jímž pachatel poškozenému hrozí, a nutí ho tak něco konat, opominout nebo trpět. Je přitom nerozhodné, zda se poškozený trestné činnosti, jejímž oznámením se hrozí, dopustil či nikoli (srov. R 27/1982).“*

4.5. Spam

Z hlediska informačních a komunikačních technologií lze obsah pojmu spam v zásadě chápat ve dvou rovinách. V **užším slova smyslu** se jedná o hromadné šíření nevyžádaného sdělení nejčastěji reklamního charakteru pomocí Internetu, nejčastěji prostřednictvím elektronické komunikace. V **širším slova smyslu** se jedná o všechny doručené nevyžádané zprávy, tedy i např. o zprávy obsahující viry, trojské koně apod.[1]

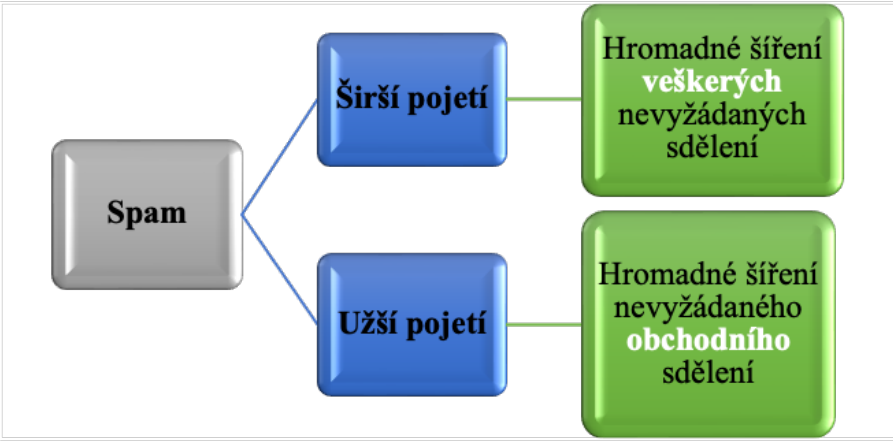


Schéma - Rozdělení spamu

Pro spam je příznačné, že se jedná o **sdělení**, které je **zaslané elektronicky, hromadně a zejména bez vyžádání.**

Spam využívá různé komunikační kanály k odesílání nevyžádaných zpráv:

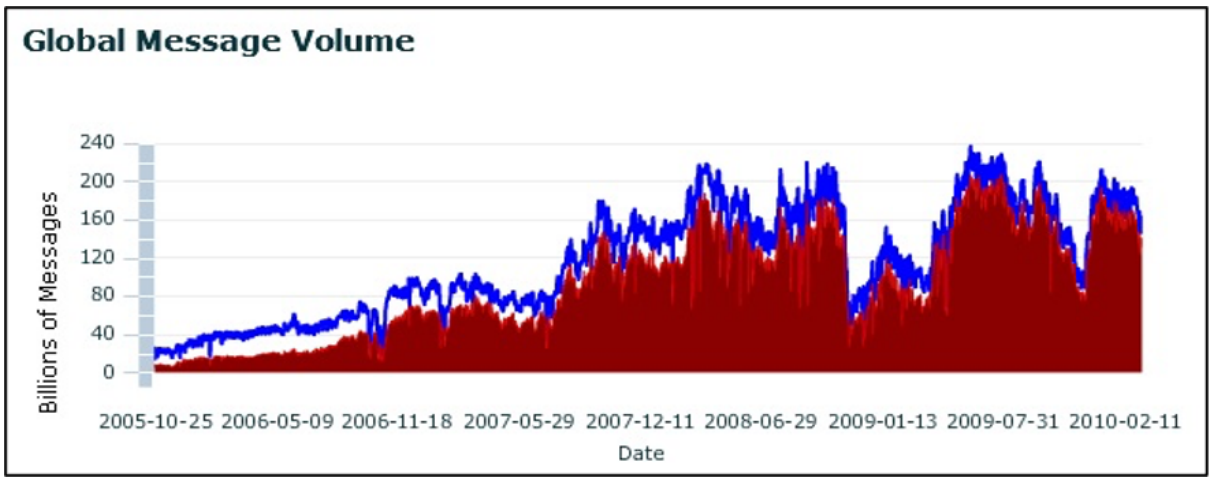
- e-mail;
- jiný messenger (ICQ, Skype atp.);
- SMS, MMS;
- diskusní fóra, blogy, sociální sítě atp.;
- herní platformy aj.

Spam může obsahovat informace:

- **obchodní či reklamní;**
- **zdraví a medicíně** (Tato kategorie obsahuje spam nabízející produkty na snížení váhy, kosmetické přípravky, netradiční medicínu, léky nedostupné v daném regionu aj.);
- **finanční** (Zejména se jedná o nabídky různých půjček možnosti přivýdělku aj.);
- **pornografické** (Tento spam buď nabízí různé, i farmaceutické přípravky na zvýšení sexuální potence, nebo odkazuje na stránky s pornografickým obsahem.);
- **edukační** (nabídky různých kurzů, tréninků aj.);
- **hoax** (řetězový dopis);
- **politické;**
- **náboženské;**
- **kriminální (do této kategorie spadají zprávy obsahující například malware, či odkazující na stránky se škodlivým kódem aj.)**

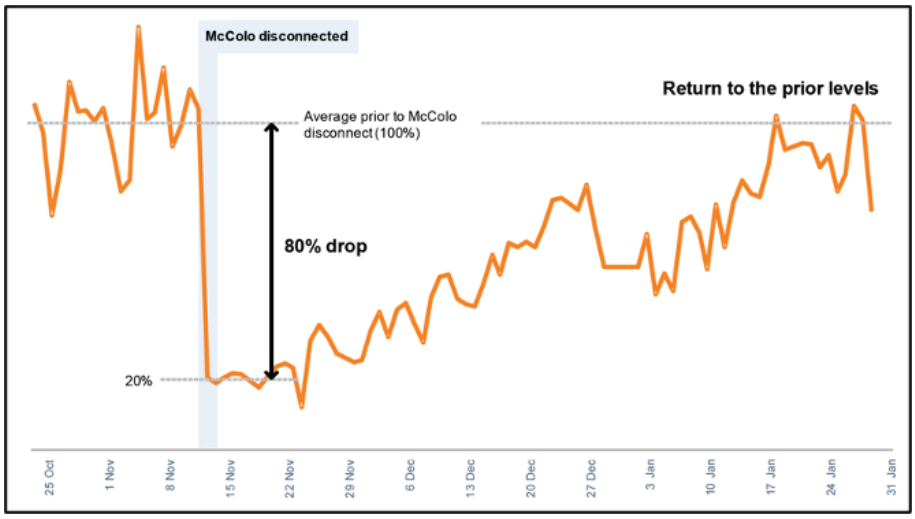
V současnosti existuje velké množství statistik uvádějících různé počty spamů v elektronických poštách. Jirovský například uvádí, že lze očekávat více než 90 % podíl spamu v elektronické poště. V roce 2006 došlo k odeslání průměrně 14,5 miliard spamových zpráv za den.[2] Díky tomu došlo i ke vzniku mnoha organizací zabývajících se spamem a poskytujících nástroje k ochraně před ním. Jednou z těchto společností byla i společnost TrustedSource[3], odkud pochází i následující graf znázorňující obsah spamu v elektronické poště od roku 2005 do roku 2010. Modrá linie znázorňuje počet e-mailových zpráv a červené pole odráží počet spamů v e-mailové poště (obojí je uvedeno v miliardách).

Bez ohledu na přesná procenta v současné době tvoří takovýto druh nevyžádaných sdělení většinu ze všech doručených e-mailových zpráv.[4]
K uživateli se však, díky řadě technických opatření na straně jednotlivých ISP, dostane minimum zpráv, jež představují spam.



Vývoj spamu od 2005 do 2010

Výrazný propad spamu na konci roku 2009 je zapříčiněn ukončením činnosti společnosti **McColo**, která se zabývala rozesíláním nevyžádaných zpráv na Internetu.[5]



Vývoj spamu po ukončení činnosti McColo v listopadu 2008

Spam zasahuje do elektronické komunikace, mnohdy ji zcela znemožní (dojde k zahlcení informační struktury) a snižuje tak důvěru společnosti v informační technologie. Pokud však dochází k omezování spamu, de facto dochází k omezování práva na svobodu projevu ve prospěch práva ochrany osobní integrity.

I z výše popsaného důvodu je právní postih spamera značně komplikovaný a v současnosti dochází k využití institutů práva občanského a správního, neboť trestní právo neumožňuje spamera potrestat.

Spam obsahující kriminální či jiný podvodný obsah je označován jako **scam** (z anglického *„scam*" – podvod, švindl). Scamy tvoří v současnosti podstatnou část spamu a jejich účelem je, typicky za použití sociálního inženýrství, získat důvěru uživatele a donutit ho vykonat požadované úkony (např. otevření přílohy e-mailu, navštívení zobrazeného URL aj.). Mezi scam je možné zařadit *phishing, malware, 419, hoax, podvodné loterie a nabídky, dárcovský scam, Cold-call Scam, Facebookový like scam aj.*

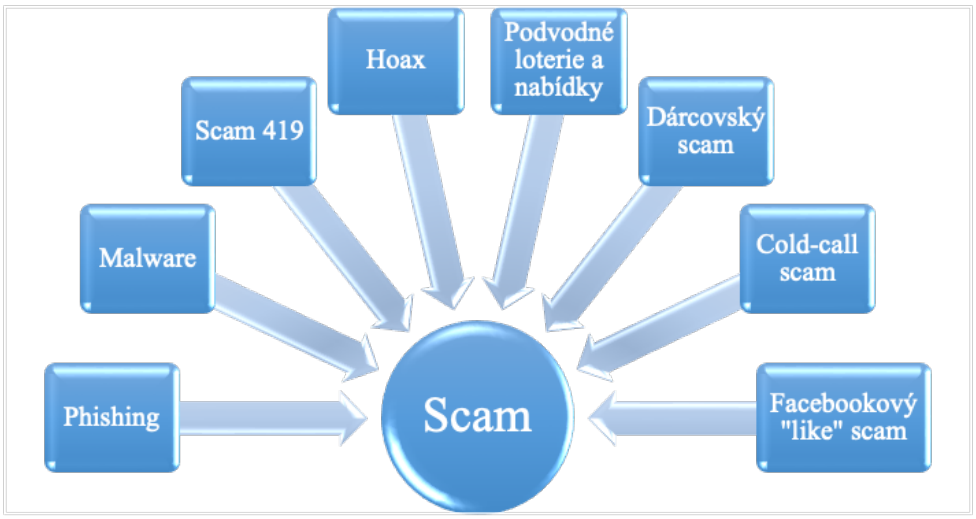


Schéma rozdělení scamu

Bližší pozornost budu na tomto místě věnovat třem typům scamu a to konkrétně **Scam 419**, **Hoax** a **Podvodným nabídkám**.

4.5.1. Scam 419

Scam 419 představuje označení pro e-maily, které jsou spíše známy jako **Nigerijské dopisy**. Tyto podvody jsou ukázkou přenosu normální kriminality (podvodů) ze světa reálného do světa virtuálního.

Pro zajímavost přikládáme tři značně odlišné zprávy mající povahu Scamu 419.

Zpráva č. 1 – „Zdědil jste obrovskou sumu peněz“

Ahoj drahý,

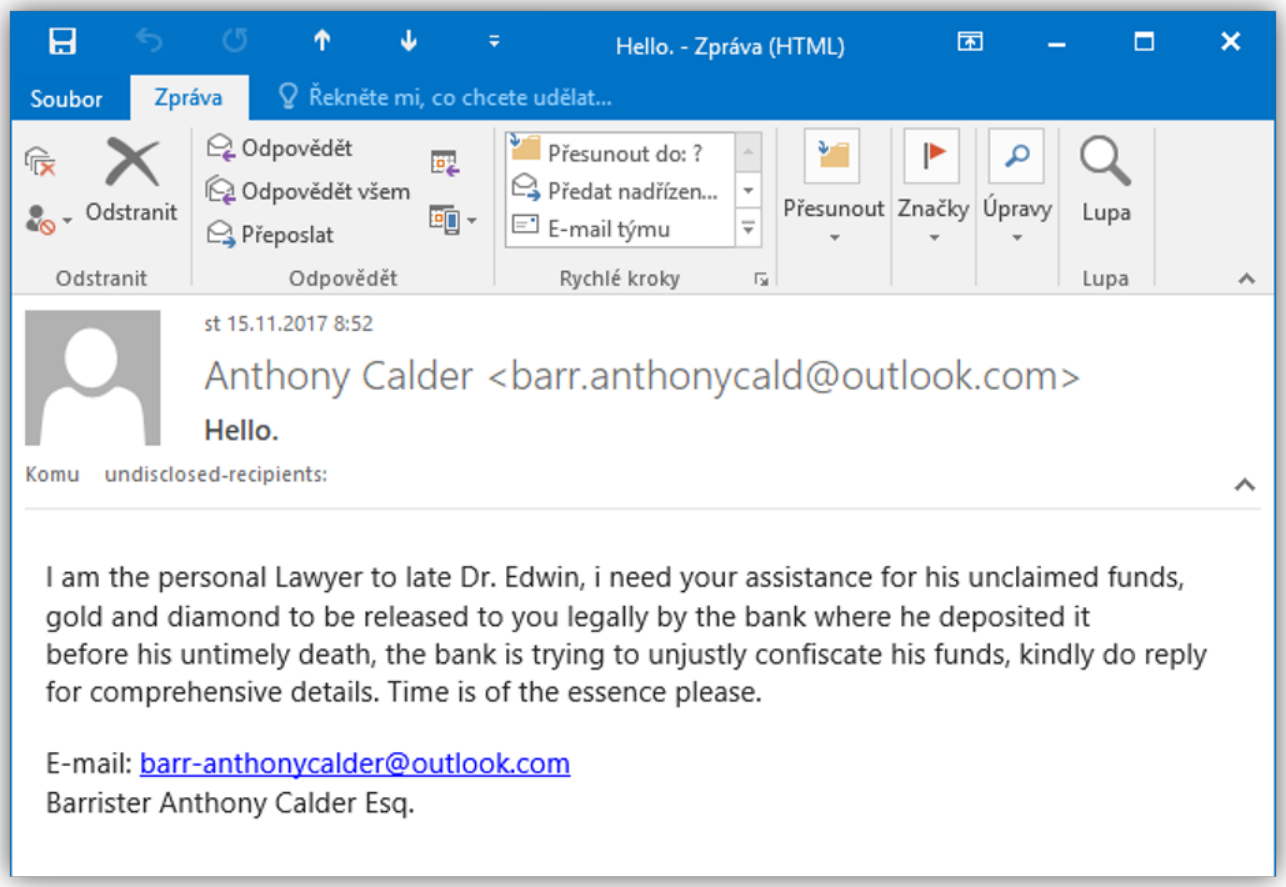
Jsem Advokát Victoria Josef, mám pro vás zprávu týkající se mého zemřelého klienta, který nese stejné příjmení jako vy, jsem si vědom, nemusí vztahovat k němu krve, ale je státním příslušníkem ve vaší zemi, který přišel o život po boku svého přímé rodina při nehodě zde v Togu motoru.

On odešel za částku ve výši 2.700.000 $, Mezitím, jeho banka chce převést výhody na některou z jeho rozšířené člena rodiny jako prezentace může být podána prostřednictvím mé kanceláře. Chcete-li být upřímný, tyto peníze patří do mého zemřelého klienta, který má stejné příjmení a státní příslušnost s vámi bydlil a působil zde v Togu pro více než 20 let jako dodavatele, ale zemřel ve smrtelné autonehody spolu se všemi členy jeho rodina v roce 2009 a nedávno, banka, kde se ukládají tyto peníze mi dal mandát k poskytnutí nějakého člena jeho rodiny požadovat tyto peníze nebo jinde to bude předána do vlády účet státní pokladny jako opuštěné peníze.

Nechci, aby se to stalo, ale problém je, že jeho předpokládaný nejbližší příbuzní zemřeli v tomto stejném autonehodě a všechny své úsilí k dohledání členy jeho rodiny, od jeho smrti byl ve sporu neúspěšný, když se nikdy představil některé z nich ke mně, zatímco on byl naživu.

Příteli, to je důvod, proč jsem se pustil na tuto misi najít někoho na práci z ruky do ruky se mnou nároku tento fond, abychom pomohli našim rodinám a potřebným, místo, aby mohly tyto zkorumpovaní vládní úředníci, aby převzal tento těžce vydělané peníze, stejně jako že a rozhazovat to, opouštět chudé masy trpět. Pro mě vyzvednout na vás mezi miliony lidí na Facebooku; prostě znamenat, že je to Bůh, který učinil naše cesta naštvaná, takže pojďme pracovat společně s jedním mysli, jak budeme sdílet peněz tak, jak jej tvrdil.
Uveďte, prosím, Váš zájem o toto tvrzení tak, že můžu vám poskytne, pokud jde o práci a směrnic.

Advokát Victoria Joseph Esq.

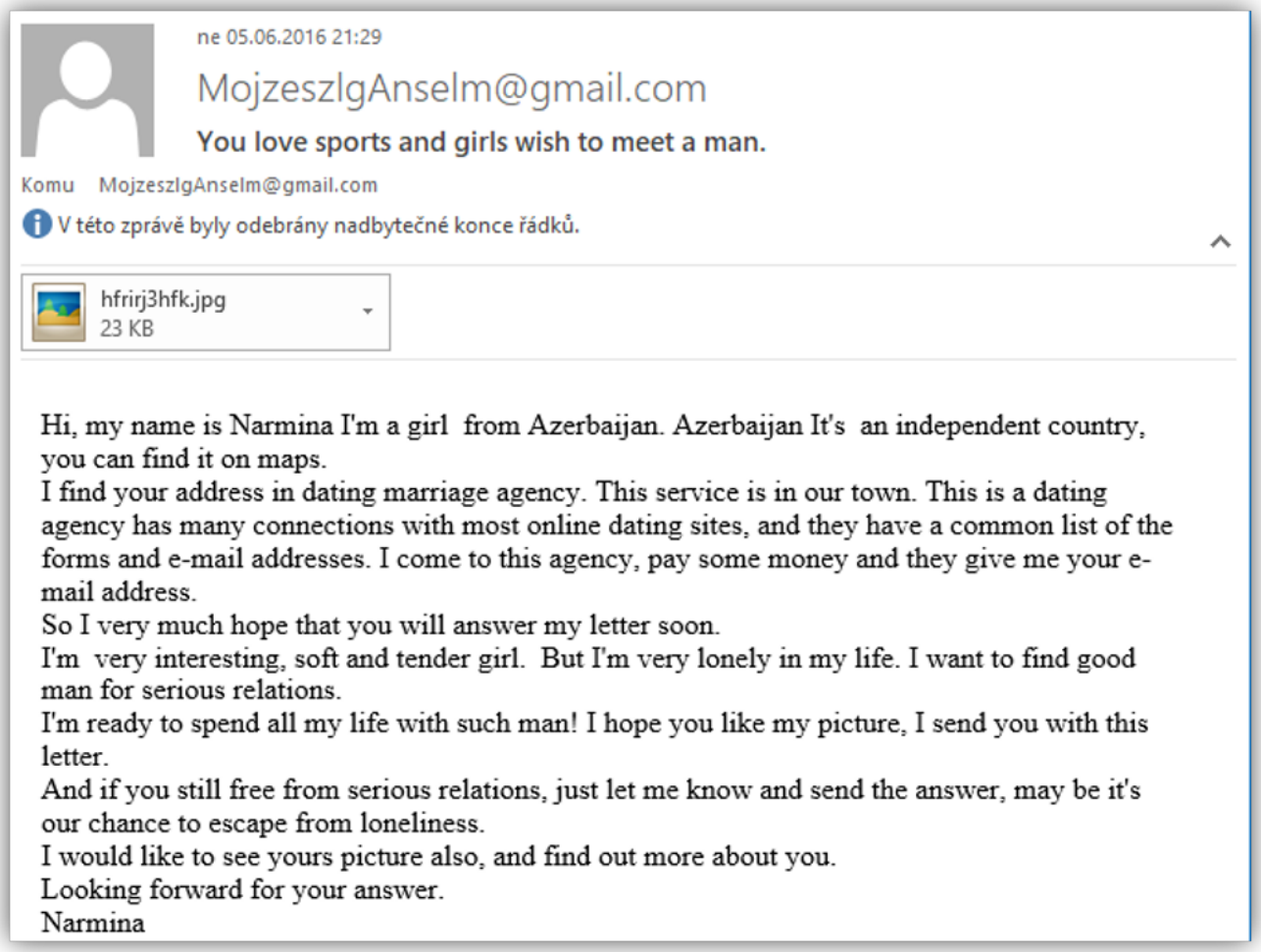


Zpráva č. 2 – „Zamilovala jsem se“

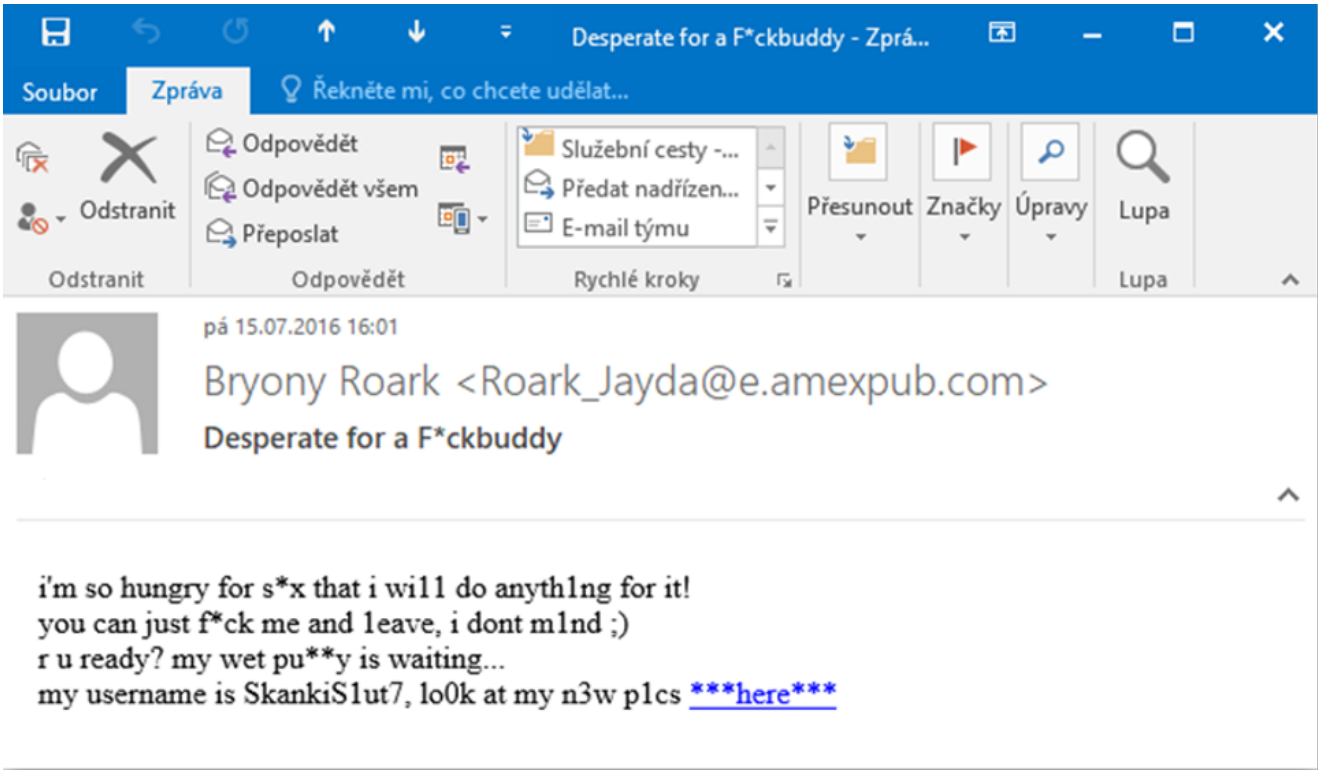
Ahoj drahoušku

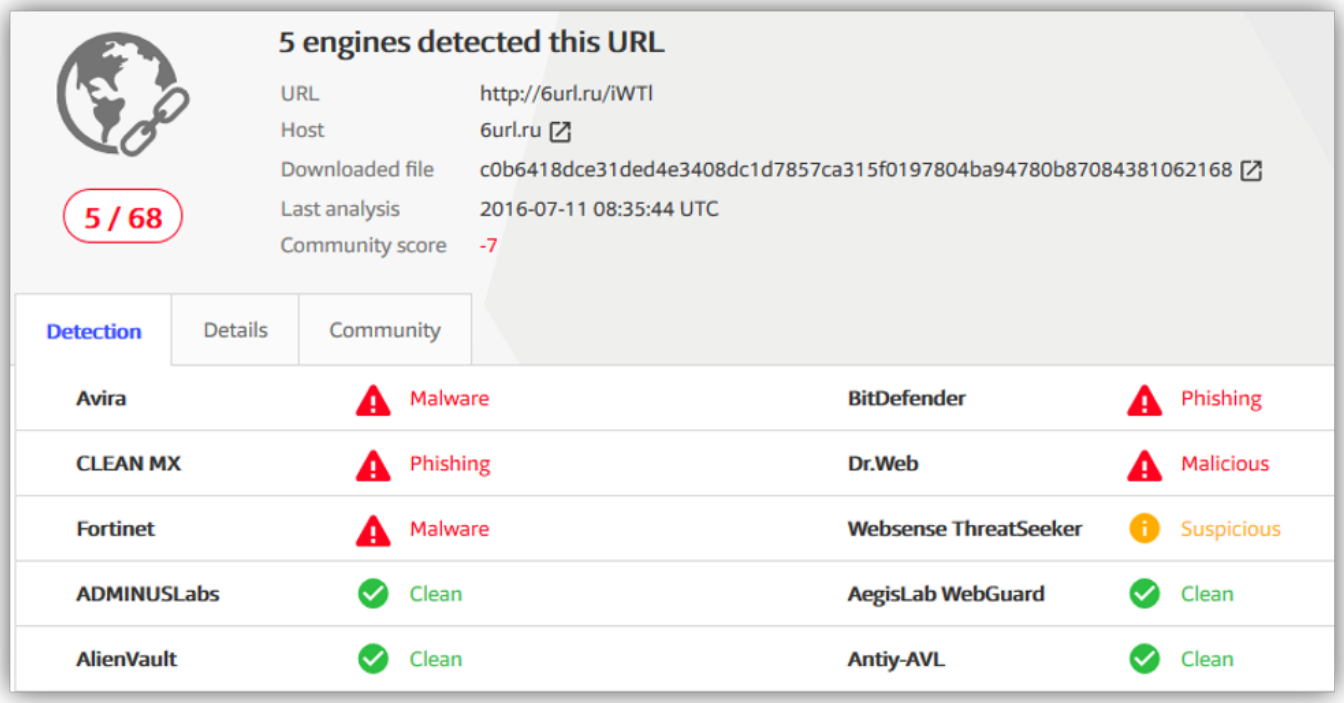
Jmenuji se Joe Anita Jsem žena, jsem zjistil jeho totožnost na straně, a chci se naučit, že víme o sobě více a sdílet společenský život s kulturou, a nemám co říct, tak prosím odpovězte mi , tak i já posílám svá data na vás a řeknu více o sobě ve svých obrazech. Děkuji mnohokrát.

Vaše radost Anita



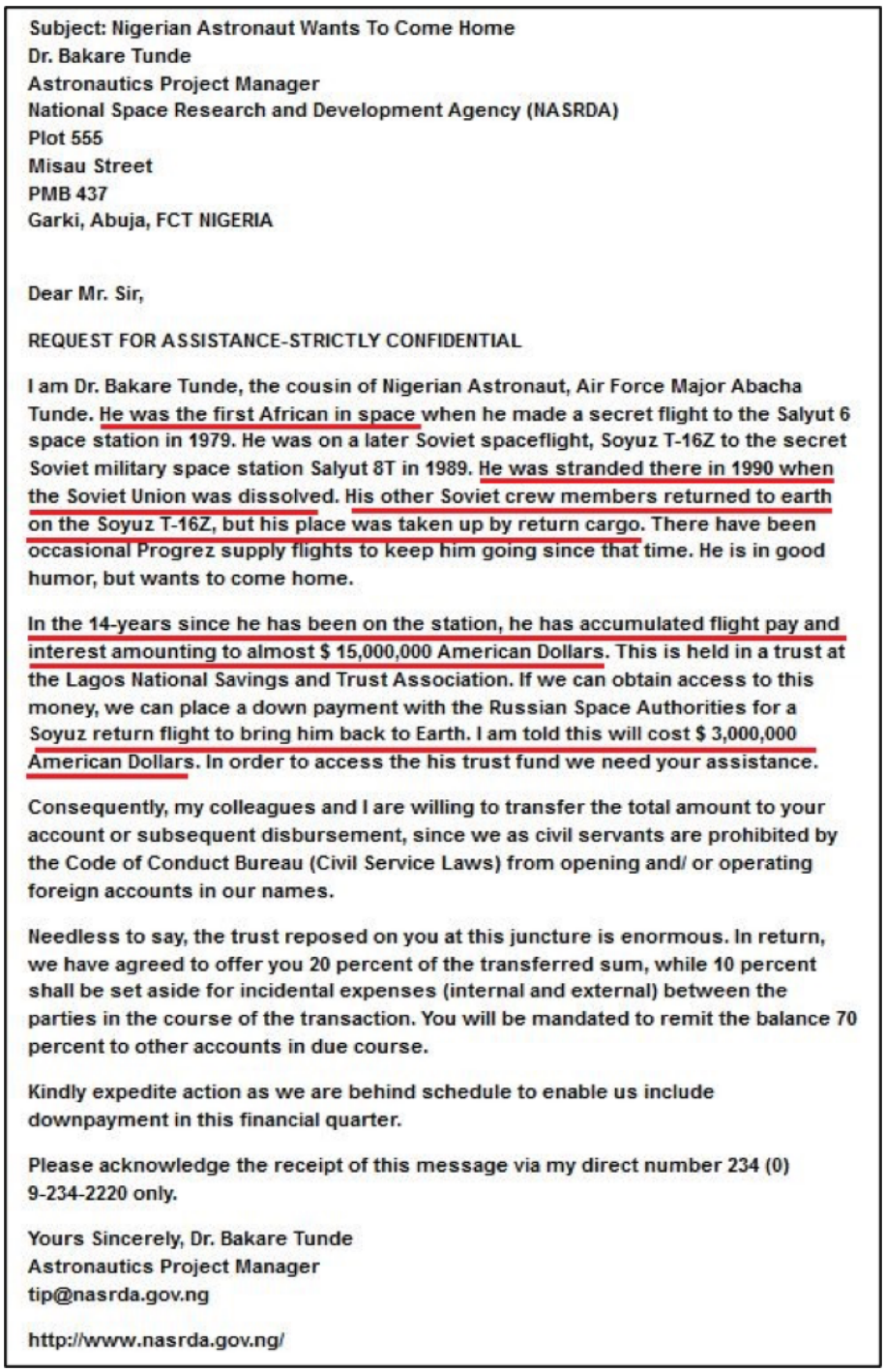
Zpráva č. 3 – „Instatntí sex“





Zpráva č. 4 – Nigerijský astronaut byl zapomenut ve vesmíru a potřebuje se dostat domů

Tato zpráva se začala šířit v roce 2004, už v té době se „první africký astronaut" nacházel ve vesmíru 14 let bez přestávky. Je třeba konstatovat, že délkou pobytu překonal všechny časy astronautů (možná i v součtu). Poslední verzi tohoto Scamu 419 jsem obdržel v r. 2016. Byť mi je tohoto imaginárního astronauta velmi líto (26 let ve vesmíru a sám), rozhodně nemíním přispět podvodníkům. Bohužel i přes zcela nesmyslný obsah a nijak nepodložené informace obsažené v tomto e-mailu se najde značná část osob, které chtějí pomoci osobě v nouzi (díky této pomoci by tento scam mohl být zařazen i do skupiny *dárcovský scam*).



Subject: Nigerian Astronaut Wants To Come Home
Dr. Bakare Tunde
Astronautics Project Manager
National Space Research and Development Agency (NASRDA)
Plot 555
Misau Street
PMB 437
Garki, Abuja, FCT NIGERIA

Dear Mr. Sir,

REQUEST FOR ASSISTANCE-STRICTLY CONFIDENTIAL

I am Dr. Bakare Tunde, the cousin of Nigerian Astronaut, Air Force Major Abacha Tunde. He was the first African in space when he made a secret flight to the Salyut 6 space station in 1979. He was on a later Soviet spaceflight, Soyuz T-16Z to the secret Soviet military space station Salyut 8T in 1989. He was stranded there in 1990 when the Soviet Union was dissolved. His other Soviet crew members returned to earth on the Soyuz T-16Z, but his place was taken up by return cargo. There have been occasional Progrez supply flights to keep him going since that time. He is in good humor, but wants to come home.

In the 14-years since he has been on the station, he has accumulated flight pay and interest amounting to almost $ 15,000,000 American Dollars. This is held in a trust at the Lagos National Savings and Trust Association. If we can obtain access to this money, we can place a down payment with the Russian Space Authorities for a Soyuz return flight to bring him back to Earth. I am told this will cost $ 3,000,000 American Dollars. In order to access the his trust fund we need your assistance.

Consequently, my colleagues and I are willing to transfer the total amount to your account or subsequent disbursement, since we as civil servants are prohibited by the Code of Conduct Bureau (Civil Service Laws) from opening and/ or operating foreign accounts in our names.

Needless to say, the trust reposed on you at this juncture is enormous. In return, we have agreed to offer you 20 percent of the transferred sum, while 10 percent shall be set aside for incidental expenses (internal and external) between the parties in the course of the transaction. You will be mandated to remit the balance 70 percent to other accounts in due course.

Kindly expedite action as we are behind schedule to enable us include downpayment in this financial quarter.

Please acknowledge the receipt of this message via my direct number 234 (0) 9-234-2220 only.

Yours Sincerely, Dr. Bakare Tunde
Astronautics Project Manager
tip@nasrda.gov.ng

http://www.nasrda.gov.ng/

Vzhledem k povaze podvodného jednání by bylo možné, v některých případech, Scam 419 označit či podřadit i pod jednání mající povahu phishingu.

4.5.2. Hoax

Hoax (anglicky - smyšlenka, žert, novinářská kachna) je další formou spamu, případně scamu. Hoax je označení pro řetězové zprávy (řetězově rozesílané zprávy typu: *„pošli to dál“*, *„pokud to nepošleš 20 dalším lidem, tak se stane…“* aj.), které uvádějí zkreslené, nepravdivé, zavádějící či jiné falešné informace. Hoax obsahuje často varování před útoky, popisy nebezpečí, prosby o pomoc, výzvy, petice, prohlášení slavných, řetězové dopisy štěstí, žertovné zprávy, obrázky a videa v prezentacích, hrající si kočičky a jiná zvířátka atd.

4.5.3. Podvodné nabídky

Velmi úspěšnou formou scamu jsou různé podvodné nabídky, které mohou být rozesílány hromadně či cíleně. V současnosti jsou takovéto nabídky rozesílány nejen prostřednictvím e-mailů, ale i pomocí jakýchkoliv instant messengerů, sociálních sítí, aukčních portálů atd.

Pokud jde o **hromadné rozesílání** podvodných nabídek, je možné si pod tímto pojmem představit celou řadu aktivit na principu „pyramida“ či „letadlo“, nabídky výhodných prací z domova[6], „zaručené“ metody zhodnocení peněz (s nejvyššími úroky), nabídky na půjčku (s nejnižšími úroky), „skvělé“ pracovní příležitosti aj.

Do **cíleného odesílání** podvodných nabídek je třeba zahrnout i jednání, které nemá povahu pouhého spamu, ale jde například o kombinaci nabídky konkrétního druhu zboží v rámci aukčních portálů a následnou komunikaci s uživateli, kteří na tuto nabídku přistoupili. Jedná se o tzv. „aukční podvody“.

Neodolatelná nabídka práce z domova (hromadné rozesílání v rámci sociální sítě Facebook)

V současnosti již rozhodně není pravidlem, že jsou hromadně či cíleně odesílané nabídky psané podezřelou nebo lámanou češtinou (nebo jsou psané anglicky či rusky), naopak snahou útočníka je přesvědčit oběť o absolutní korektnosti, serióznosti a „čestnosti" svého jednání. V rámci aukčních portálů jsou velmi často podvodně nabízeny různé druhy elektroniky, zejména mobilních telefonů a počítačů. Vlastní podvodné jednání pak může spočívat například ve změně podstatných informací [např. země původu mobilního telefonu; informaci o tom, že jde o kopii (padělek) telefonu] či nedoručení zboží jako takového (útočník velmi často žádá zaplacení celé částky či zálohy).

Nápaditost útočníků je v prostředí Internetu značná a v případě jakýchkoli nabídek, inzerce a zejména zasílání záloh či plateb je vhodné být paranoidní a nedůvěřovat neznámým osobám.

V případě podvodných nabídek, kdy se útočník snaží získat různé zálohy či jiné platby předem, je takovéto jednání možné postihnout dle **§ 209** (Podvod) TZK.

Možnosti trestněprávního postihu v ČR

Pokud jde o trestněprávní postih spamu a spammerů, v České republice není v současnosti zcela (vy)řešený. Absentuje jak vnitrostátní, tak i mezinárodněprávní ochrana před tímto nežádoucím jednáním. Ani Úmluva o kyberkriminalitě v sobě neobsahuje vymezení spamu jako trestného činu.

Například v **USA** již v minulosti k odsouzení spammerů[7] za rozesílání nevyžádané pošty došlo. Například **Jeremy Jaynes** byl v roce 2007 odsouzen soudem ve Virginii k 9-letému trestu odnětí svobody. Obviněn byl již v roce 2003, jako důkaz sloužilo 53 000 spamů odeslaných během tří dnů. Prokurátor však dle svého vyjádření věří, že Jaynes je odpovědný za rozesílání více než 10.000.000 spamů denně, což mu mělo vynést přibližně 750.000 USD měsíčně.

Vzhledem k tomu, že pod pojmem spamming nelze zařadit pouze jednu formu škodlivého jednání, je velmi složité spamming sám o sobě postihnout prostředky trestního práva. Tak lze učinit pouze u jednotlivých jeho druhů. V určitých případech připadá v úvahu postihnout sběr e-mailových adres, jestliže takový sběr naplní znaky skutkové podstaty trestného činu neoprávněného nakládání s osobními údaji podle **§ 180** (Neoprávněné nakládání s osobními údaji) TZK. Pokud spam obsahuje malware, nebo je jeho cílem dokonání podvodného jednání, je možné činnost spamera postihnout dle ustanovení vztahujících se na malware či na phishing.

---

[1] Ke třídění spamu srov. např. GONZÁLES-TALAVÁN, Guillermo. A Simple, Configurable SMTP Anti-spam Filter: Greylists. *Computers & Security*, 2006, roč. 25, č. 3, s. 229 – 236.

[2] Srov. např. *Spam statistics*. [online]. [cit.14.8.2016]. Dostupné z: https://www.spamcop.net/spamstats.shtml

Spam Statistics and Facts. [online]. [cit.14.8.2016]. Dostupné z: http://www.spamlaws.com/spam-stats.html

[3] Původní online zdroj: http://www.trustedsource.org/TS?do=home [cit.12.2.2010].

[4] Nelze přesně určit, kolik procent ze všech e-mailů tvoří spam. Různé dostupné zdroje uvádějí různá, někdy značně odlišná čísla. Např. jeden z poskytovatelů antispamových řešení, společnost POSTINI, v březnu 2005 v průběhu 24 hodin zaznamenala, že 10 z 12 e-mailů bylo spam. K četnosti zasílání spamu srov. např. LANCE, James. *Phishing bez záhad*. Praha: Grada, 2007, s. 22, SCHRYEN, Guido. The Impact that Placing Email Addresses on the Internet Has on the Receipt of Spam: An Empirical Analysis. *Computers & Security*, 2007, roč. 26, č. 5, s. 361 – 372.

[5] *Malware, mayhem, and the McColo takedown.* [online]. [cit.14.8.2016]. Dostupné z: http://betanews.com/2008/11/13/malware-mayhem-and-the-mccolo-takedown/

[6] Tyto nabídky mohou jednak spočívat v žádosti typu: *„pošlete nám 10 dolarů na účet a my vám pošleme návod, jak vydělat 8847 dolarů měsíčně“*. Druhou možností je, že tyto nabídky práce nevyžadují žádný poplatek předem, pouze požadují registraci uživatele. Vlastní registrací pak útočník obdrží osobní údaje o uživateli. Na uživatelovu e-mailovou adresu pak může být zaslán e-mail od této společnosti, obsahující např. malware aj.

[7] *Convicted spammer challenging Va. law* [online]. [cit.14.8.2016]. Dostupné z: http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va_N.htm

Top Spammer Sentenced to Nearly Four Years. [online]. [cit.14.8.2016]. Dostupné z: http://www.pcworld.com/article/148780/spam.html

Buffalo Spammer jde na 7 let za mříže kvůli rozesílání nevyžádané pošty. [online]. [cit.14.8.2016]. Dostupné z: http://technet.idnes.cz/buffalo-spammer-jde-na-7-let-za-mrize-kvuli-rozesilani-nevyzadane-posty-13i-/tec_reportaze.aspx?c=A040528_28629_tec_aktuality

4.6. Phishing, Pharming, Spear Phishing, Vishing, Smishing

4.6.1. Phishing

Pojmem phishing se nejčastěji označuje podvodné či klamavé jednání, jehož cílem je získat informace o uživateli, jako jsou např. uživatelské jméno, heslo, číslo kreditní karty, PIN aj.

V **užším slova smyslu** phishing představuje jednání, které po uživateli vyžaduje navštívení podvodné stránky (zobrazující např. webovou stránku internetového bankovnictví, online obchodu aj.) a následné vyplnění „přihlašovacích informací", případně jsou tyto informace vyžadovány přímo (např. při vyplnění formuláře aj.).

V **širším slova smyslu** se za phishing dá označit jakékoli podvodné jednání, které má v uživateli vzbudit důvěru, snížit jeho ostražitost či jej jinak donutit akceptovat scénář předem připravený útočníkem. V tomto širším slova smyslu již není po uživateli požadováno vyplňování údajů, avšak je mu doručena zpráva (či je uživatel přesměrován na stránku) typicky obsahující malware, který si uvedené údaje posbírá sám. Dále do tohoto širšího pojetí mohou být zařazeny i dárcovské scamy atp.

V obou dvou případech dochází k oklamání uživatele, který je cílem phishingového útoku, rozdíl spočívá především v tom, jaká míra interakce je po uživateli vyžadována.

Podstatou phishingu je využívání sociálního inženýrství. Phishing je možné provádět i ve světě reálném (viz podvody aj.), avšak svět virtuální umožňuje útočníkovi rozesílat podvodné zprávy obrovskému množství potenciálních obětí s minimem námahy. Phishing je, se značnou mírou nadsázky, možné přirovnat ke *„kobercovému bombardování"*. Stejně jako v případě bombardování phishing cílí na relativně neurčené množství obětí proto, aby měl útočník naději na úspěch. Google např. v roce 2014 uváděl, že scam mající povahu skutečně dobrého phishingu je při zisku dat o uživatelích úspěšný z 45%.[1]

Phishing není zaměřen pouze na e-maily. Je možné nalézt phishing v rámci instant messages (Skype, ICQ, Jabber aj.), sociálních sítí, SMS a MMS zpráv, chatovacích místností, scamu (podvodné nabídky práce, zboží aj.), falešných aplikací do prohlížeče[2] aj.

Phishing v užším smyslu slova

Princip *„klasického"* phishingového útoku spočívá nejčastěji v zaslání tzv. phishingového e-mailu poškozenému, který na první pohled nevzbuzuje žádné podezření, že by mělo jít o podvodné sdělení. Součástí takového e-mailu bývá zpravidla odkaz, na nějž je uživatel vyzýván kliknout.

Po kliknutí na přiložený odkaz se uživatel dostává na podvodnou webovou stránku, která se svým vzhledem i funkcemi od originální korektní webové schránky téměř neliší. Jedná-li se o napodobeninu webové stránky, pomocí které je možné realizovat platební styk, vstupovat na zabezpečená konta, taková konta spravovat apod., pak jsou uživatelem zadaná data automaticky odesílána útočníkovi.[3] Ten tímto způsobem může získat identifikační údaje uživatelů internetových bankovních služeb, přístup k jednotlivým bankovním účtům uživatelů napadených systémů, může získat identifikační čísla a další údaje o platebních kartách, s jejichž pomocí je poté v prostředí Internetu možné realizovat platební styk atd.

Vlastní phishingový útok probíhá v několika krocích.[4]

1. **Plánování phishingového útoku**

V této fázi phishingového útoku dochází k výběru cíle (skupiny uživatelů) a k výběru metody, která má být k útoku použita. Je vyhodnocováno, jakým způsobem je cíl technicky zabezpečen, jaká jsou rizika odhalení identity útočníka apod.

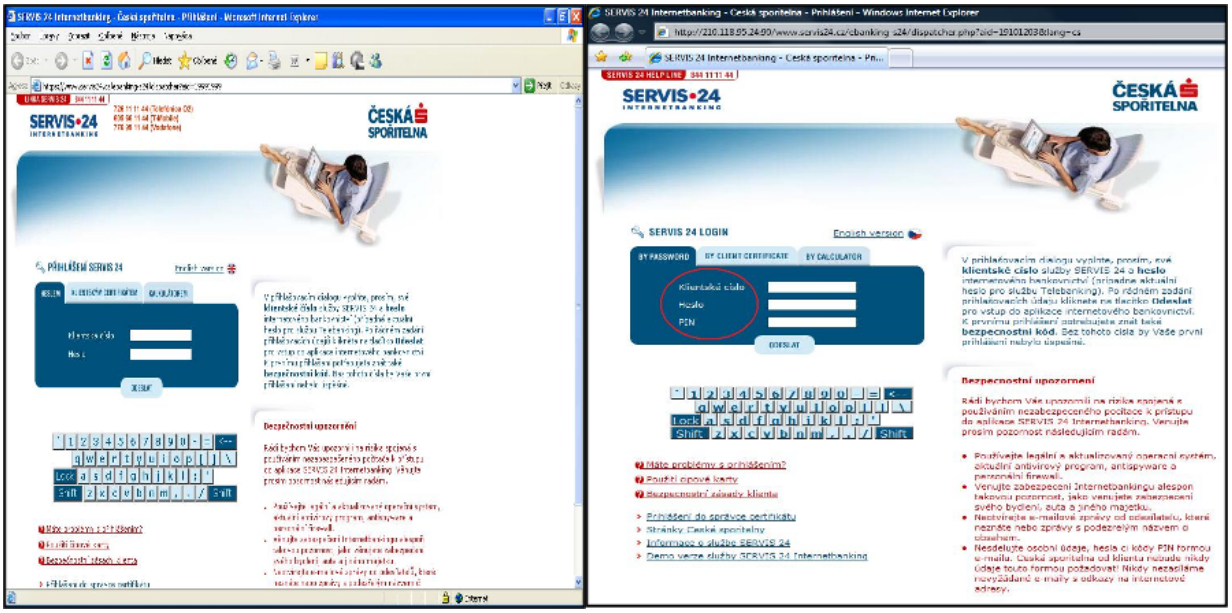
2. **Vytváření podmínek pro phishingový útok**

V této fázi dochází k technickému řešení phishingového útoku. Útočník získává seznamy e-mailových adres uživatelů, jimž má být zaslán phishingový e-mail, je vytvořená datová schránka, kam systém zašle získaná data uživatelů, dochází k vytvoření důvěryhodného sdělení, které je následně distribuováno uživatelům.

3. **Vlastní phishingový útok**

Phishingový e-mail je doručen jednotlivým uživatelům a v závislosti na kvalitě zpracování tohoto e-mailu a dalších faktorech (zkušenost uživatele, jeho informovanost o phishingové problematice, antiphinshingový software cíle apod.) jsou data zasílána do datové schránky útočníka. V této fázi phishingového útoku se vůbec poprvé uživatel setkává s phishingovým e-mailem.

Jako záminka často slouží informace o chybě v bezpečnostním systému společnosti či jiné varování, které má vzbudit u uživatele pocit autentičnosti této zprávy. Po aktivaci interaktivního odkazu je osoba přesměrována na webovou stránku, vytvořenou útočníkem, věrně kopírující originální stránku finanční instituce. Uživatel je vyzván k vyplnění přihlašovacích údajů, zpravidla včetně čísla karty a PIN kódu. Vyplněné údaje jsou odeslány na adresu phishera, který následně odčerpá z účtu část či veškeré finanční prostředky a způsobí tím klientovi škodu (viz následující obrázek).



Originální stránka (vlevo) a podvodná stránka (vpravo)

4. **Sběr dat**

Útočník získává data, která v prostředí falešné webové stránky zadali jednotliví uživatelé napadeného systému.

5. **Odčerpání peněžních prostředků či jiný profit z phishingového útoku**

Útočník pomocí získaných dat vstupuje na skutečná bankovní konta jednotlivých uživatelů a odčerpává peněžní prostředky. Pomocí převodu na další, zejména zahraniční účty, rozmělnění těchto peněžních prostředků a pomocí dalších technik se odčerpané peněžní prostředky stávají prakticky nevystopovatelnými.

Je velmi obtížné určit, kolik phishingových útoků je denně po celém světě realizováno. Stejně tak je problematické určit, kolik klientů napadených společností odpoví na phishingový e-mail. Odhaduje se, že míra návratnosti se pohybuje kolem 0,01 a 0,1 %.[5]

Prognózy v roce 2007 odhadovaly, že „klasických" phishingových podvodů či kampaní bude v budoucnu přibývat.[6] Tyto prognózy se naplnily částečně, neboť ubývá „klasických" phishingových kampaní, avšak phishing v širším slova smyslu je na vzestupu[7], zejména se objevují jeho nové modifikace či propojení phishingu s jinými typy útoků (malware, propojení do sítě botnet aj.).

Phishing v širším smyslu slova

V rámci demonstrace phishingu v širším slova smyslu uvedu čtyři kampaně, které proběhly v České republice a byly více či méně úspěšné. Uvedené útoky samozřejmě nejsou jedinými phishingovými útoky v širším slova smyslu, které se v ČR uskutečnily. Důvodem výběru těchto čtyř konkrétních útoků je ta skutečnost, že chci poukázat zejména na inovativní přístup útočníka a vhodné spojení technického útoku se sociálním inženýrstvím. Konkrétně se jedná o útoky:

1. **Dluh/Banka/Exekuce**
2. **Česká pošta**
3. **Vánoce a dárky**
4. **Seznam.cz – One Time Password**

4.6.1.1. Dluh/Banka/Exekuce[8]

Phishingová kampaň pracovně nazvaná DBE zasáhla Českou republiku v masivním rozsahu v roce 2014 (přičemž dozvuky této kampaně přetrvaly minimálně do konce roku 2015).[9] Vlastní útok byl velice precizně připraven a zahrnoval v sobě jak vlastní phishing, tak distribuci malware (do počítače a mobilního zařízení). Celý útok je možné rozdělit do následujících fází:

1. **Phishingová kampaň**
2. **Instalace malware do počítače**
3. **Přístup k online bankovnictví**
4. **Instalace malware do mobilního zařízení**
5. **Převod a odčerpání finančních prostředků**

Ad 1) **Phishingová kampaň**

Prvním předpokladem pro to, aby útočníci mohli úspěšně získat finanční prostředky, byla velká phishingová kampaň, na kterou by zareagoval dostatečný

počet osob. Vlastní rozesílání podvodných e-mailů bylo rozloženo do tří po sobě jdoucích vln phishingových zpráv:

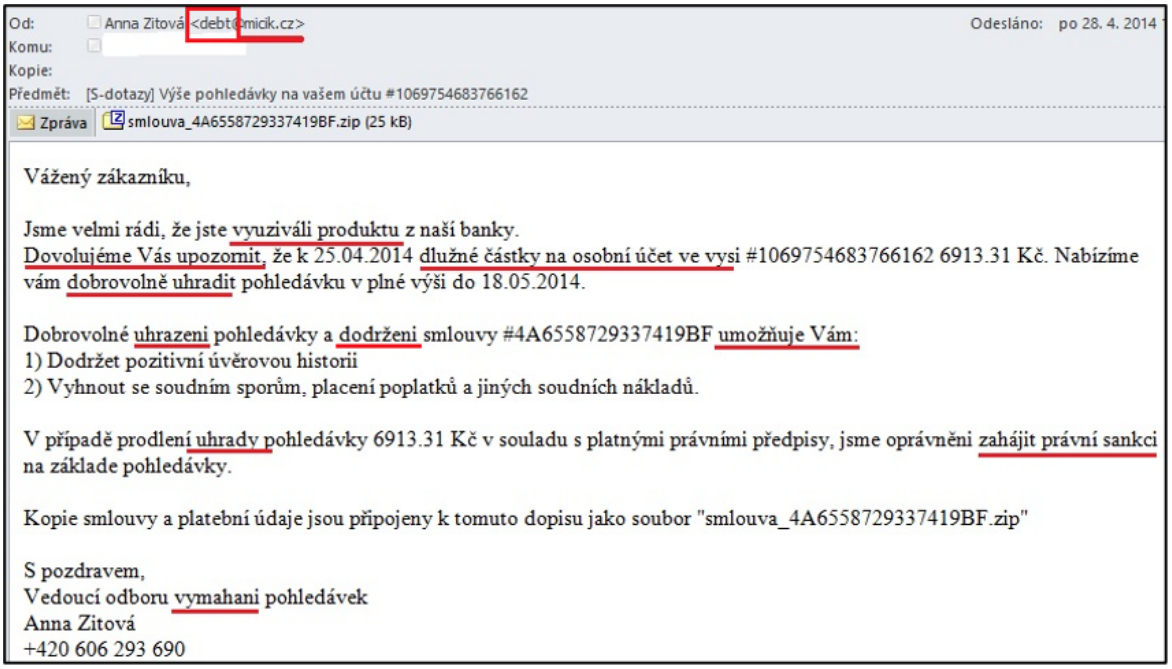
I. **Dluh** (debt@....); březen - duben 2014

II. **Banka** (bank@....); květen - červen 2014

III. **Exekuce** (emissions@...); červenec - září 2014

V rámci jednotlivých kampaní docházelo k zvyšování „kvality" vlastních e-mailových zpráv a zejména lepšímu využití sociálního inženýrství ve vztahu k předpokládaným obětem v cílovém regionu, tedy ČR. Všechny výše uvedené phishingové kampaně však měly minimálně dva společné znaky. Za prvé se jednalo o tu skutečnost, že v příloze rozeslaného e-mailu se vždy nacházel soubor, tvářící se jako textový dokument, avšak jednalo se o spustitelný soubor, konkrétně malware: Trojan.[10] Druhým společným znakem bylo, že sociální inženýrství využívalo obav oslovených jedinců z případných soudních sporů, v posledním případě z exekuce.

První vlna phishingových útoků používala velmi špatnou češtinu, byla rozesílána z různých, pokud se jedná o vymáhání pohledávky ne zcela důvěryhodných domén registrovaných v ČR (např. micik.cz či dhome.cz aj.). Využívána byla různá jména osob a existující telefonní čísla, dohledatelná na Internetu (osoba vlastnící toto číslo pak s vlastním útokem neměla nic společného).



Od: Anna Zitová <debt@micik.cz> Odesláno: po 28. 4. 2014
Komu:
Kopie:
Předmět: [S-dotazy] Výše pohledávky na vašem účtu #1069754683766162
Zpráva smlouva_4A6558729337419BF.zip (25 kB)

Vážený zákazníku,

Jsme velmi rádi, že jste využiváli produktu z naší banky.
Dovolujéme Vás upozornit, že k 25.04.2014 dlužné částky na osobní účet ve vysi #1069754683766162 6913.31 Kč. Nabízíme vám dobrovolně uhradit pohledávku v plné výši do 18.05.2014.

Dobrovolné uhrazeni pohledávky a dodrženi smlouvy #4A6558729337419BF umožňuje Vám:
1) Dodržet pozitivní úvěrovou historii
2) Vyhnout se soudním sporům, placení poplatků a jiných soudních nákladů.

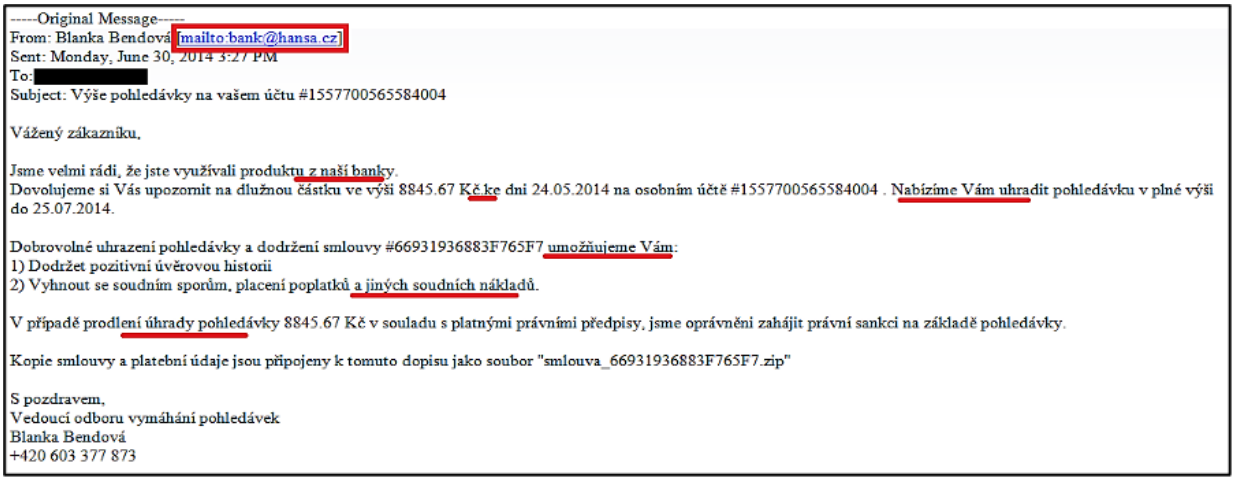
V případě prodlení uhrady pohledávky 6913.31 Kč v souladu s platnými právními předpisy, jsme oprávněni zahájit právní sankci na základe pohledávky.

Kopie smlouvy a platební údaje jsou připojeny k tomuto dopisu jako soubor "smlouva_4A6558729337419BF.zip"

S pozdravem,
Vedoucí odboru vymahani pohledávek
Anna Zitová
+420 606 293 690

Podvodný e-mail rozeslaný v rámci vlny Dluh

V rámci druhé vlny došlo k zlepšení používané češtiny.



-----Original Message-----
From: Blanka Bendová [mailto:bank@hansa.cz]
Sent: Monday, June 30, 2014 3:27 PM
To: [redacted]
Subject: Výše pohledávky na vašem účtu #1557700565584004

Vážený zákazníku,

Jsme velmi rádi, že jste využívali produktu z naší banky.
Dovolujeme si Vás upozornit na dlužnou částku ve výši 8845.67 Kč ke dni 24.05.2014 na osobním účtě #1557700565584004 . Nabízíme Vám uhradit pohledávku v plné výši do 25.07.2014.

Dobrovolné uhrazení pohledávky a dodržení smlouvy #669319368883F765F7 umožňujeme Vám:
1) Dodržet pozitivní úvěrovou historii
2) Vyhnout se soudním sporům, placení poplatků a jiných soudních nákladů.

V případě prodlení úhrady pohledávky 8845.67 Kč v souladu s platnými právními předpisy, jsme oprávněni zahájit právní sankci na základě pohledávky.

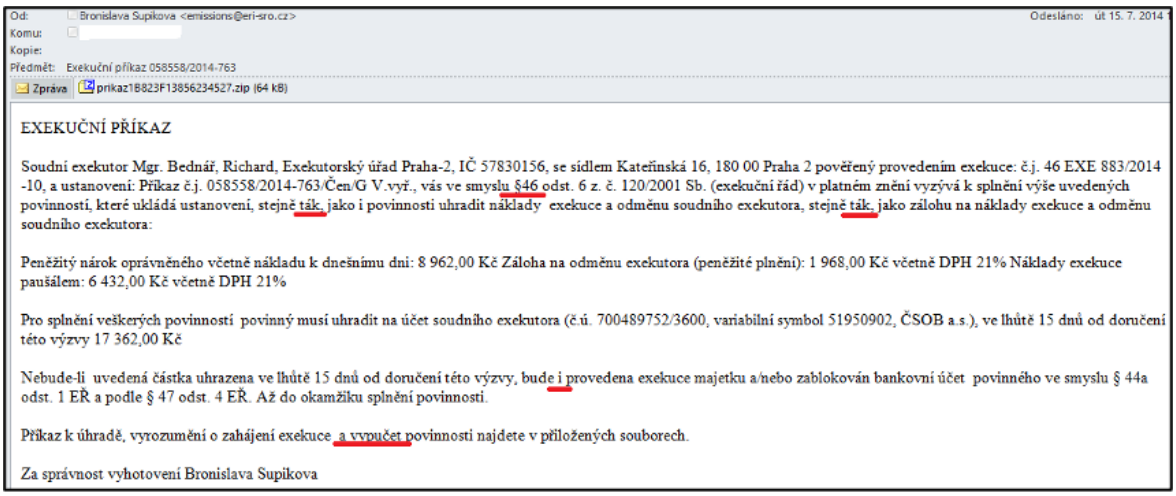
Kopie smlouvy a platební údaje jsou připojeny k tomuto dopisu jako soubor "smlouva_669319368883F765F7.zip"

S pozdravem,
Vedoucí odboru vymáhání pohledávek
Blanka Bendová
+420 603 377 873

Podvodný e-mail rozeslaný v rámci vlny Banka

V době, kdy se začaly tyto phishingové útoky objevovat, zveřejňovaly nejrůznější bezpečnostní organizace a CSIRT[11] týmy, ale i masmédia varování, včetně uvedení návodů, jak k takovýmto zprávám přistupovat.[12]

Obě kampaně byly relativně úspěšné, avšak nejúspěšnější byl útok, kde podvodný e-mail představoval varování (výzvu) od exekutora.


Od: Bronislava Supikova <emissions@eri-sro.cz> Odesláno: út 15. 7. 2014
Komu:
Kopie:
Předmět: Exekuční příkaz 058558/2014-763
Zpráva prikaz1B823F13856234527.zip (64 kB)

EXEKUČNÍ PŘÍKAZ

Soudní exekutor Mgr. Bednář, Richard, Exekutorský úřad Praha-2, IČ 57830156, se sídlem Kateřinská 16, 180 00 Praha 2 pověřený provedením exekuce: č.j. 46 EXE 883/2014 -10, a ustanovení: Příkaz č.j. 058558/2014-763/Čen/G V.vyř., vás ve smyslu §46 odst. 6 z. č. 120/2001 Sb. (exekuční řád) v platném znění vyzývá k splnění výše uvedených povinností, které ukládá ustanovení, stejně ták, jako i povinnosti uhradit náklady exekuce a odměnu soudního exekutora, stejně ták, jako zálohu na náklady exekuce a odměnu soudního exekutora:

Peněžitý nárok oprávněného včetně nákladu k dnešnímu dni: 8 962,00 Kč Záloha na odměnu exekutora (peněžité plnění): 1 968,00 Kč včetně DPH 21% Náklady exekuce paušálem: 6 432,00 Kč včetně DPH 21%

Pro splnění veškerých povinností povinný musí uhradit na účet soudního exekutora (č.ú. 700489752/3600, variabilní symbol 51950902, ČSOB a.s.), ve lhůtě 15 dnů od doručení této výzvy 17 362,00 Kč

Nebude-li uvedená částka uhrazena ve lhůtě 15 dnů od doručení této výzvy, bude i provedena exekuce majetku a/nebo zablokován bankovní účet povinného ve smyslu § 44a odst. 1 ER a podle § 47 odst. 4 ER. Až do okamžiku splnění povinnosti.

Příkaz k úhradě, vyrozumění o zahájení exekuce a vypučet povinnosti najdete v přiložených souborech.

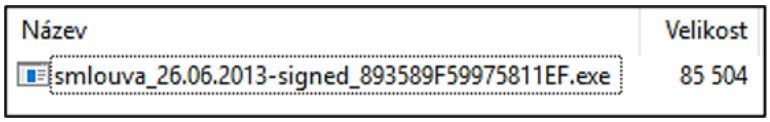
Za správnost vyhotovení Bronislava Supikova

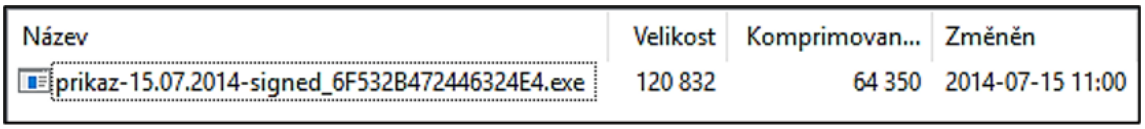
Podvodný e-mail rozeslaný v rámci vlny Exekuce

Čeština použitá v „exekučním příkazu" obsahovala zejména chyby v diakritice, případně byly poněkud krkolomněji formulovány některé věty (podtrženy jsou nejvíce patrné chyby). Využívána však byla jména skutečných exekutorů, dohledatelná na Internetu (uvedený exekutor pak s vlastním útokem neměl nic společného), stejně jako reálně se tvářící čísla exekucí.

Ad 2) Instalace malware do počítače

Jak již bylo uvedeno dříve, všechny phishingové kampaně obsahovaly v příloze rozeslaného e-mailu malware: TrojanDownloader (tedy malware určený ke stahování dalšího malware). Tento malware byl primárně vytvořen a zacílen na operační systém Windows XP, kterému v březnu 2014 skončila podpora.





Spustitelný soubor (malware) obsažený v příloze podvodných e-mailů

Po spuštění přílohy došlo k instalaci malware (bankovní trojský kůň) *„Tinba"*, který byl na pozadí stažen z Internetu, zatímco uživateli byla zobrazena smlouva či exekuční příkaz v textovém editoru.[13]

Malware se zapsal do adresáře: **Users/***konkrétní uživatel***/AppData/Roaming/brothel**. V tomto adresáři bylo možné nalézt ate.exe, což je soubor, který vznikl po otevření spustitelného souboru v phishingovém e-mailu. Zároveň byl v registrech vytvořen příslušný klíč ve větvi **HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRun**. Tímto způsobem bylo možné ověřit, zda se jedná o malware pocházející z tohoto útoku.

Ad 3) Přístup k online bankovnictví

Dalším krokem útočníka pak bylo počkat na okamžik, kdy se oběť přihlásí do online bankovnictví. Malware v počítači je schopen zaznamenávat komunikaci mezi uživatelem a online bankovnictvím a útočník má možnost tuto komunikaci sledovat. Uživatel měl minimální šanci rozpoznat vlastní útok, neboť URL adresa v prohlížeči náležela dané bance a komunikace byla zabezpečena (HTTPS).

„Vlastní kradení citlivých dat probíhá vložením škodlivého kódu do oficiálních stránek bank. Konfigurační skripty jsou staženy z C&C serverů (stroje patřící útočníkům, sloužící pro ovládání botnetu) a dešifrovány výše zmíněným způsobem. Zajímavostí je znovupoužití stejného formátu konfiguračních souborů známých bankovních trojanů Carberp a Spyeye. Pro každé botuid (unikátní hodnota, která identifikuje prostředí uživatele) se uloží seznam uživatelských jmen a hesel na C&C serveru. Další skripty jsou stahovány v závislosti na použité bance, buď tedy ***hXXps://andry-shop.com/gate/get_html.js;hXXps://andry-shop.com/csob/gate/get_html.js;*** *resp.* ***hXXps://yourfashionstore.net/panel/a5kGcvBqtV,*** *které se stáhnou, pokud oběť navštíví webové stránky České spořitelny, ČSOB, resp. Fia."* ***[14]***

Ad 4) Instalace malware do mobilního zařízení

Dalším krokem útočníka bylo přesvědčit uživatele o nutnosti zvýšení zabezpečení, při přístupu k online bankovnictví. Důvodem varování, které vydala údajná banka (ve skutečnosti se jednalo o webovou stránku ovládanou útočníkem), bylo „zvýšení" bezpečnosti spojení. Oběti byla nabídnuta stránka s volbou operačního systému mobilního zařízení (OS Android, Windows Phone, Blackberry i iPhone), avšak pouze verze pro Android umožnil stažení malware do telefonu. Útočníci volili různé způsoby distribuce malware do telefonu, od prostého zaslání SMS zprávy s odkazem, ze kterého si uživatel měl daný program stáhnout, po zaslání SMS zprávy a QR kódu.[15]

Malware stažený a nainstalovaný do mobilního zařízení byl společností Avast! detekován jako Android: *Perkele-T*.

Tento malware měl za cíl získat přístup a plnou kontrolu nad druhotným autentizačním prostředkem (dvoufaktorová autentizace), kterým je ve většině případů právě mobilní telefon. V případě, že uživatel využíval jiný operační systém než Android, byla mu zobrazena zpráva: *„Zkuste to prosím později“*.

Ad 5) Převod a odčerpání finančních prostředků

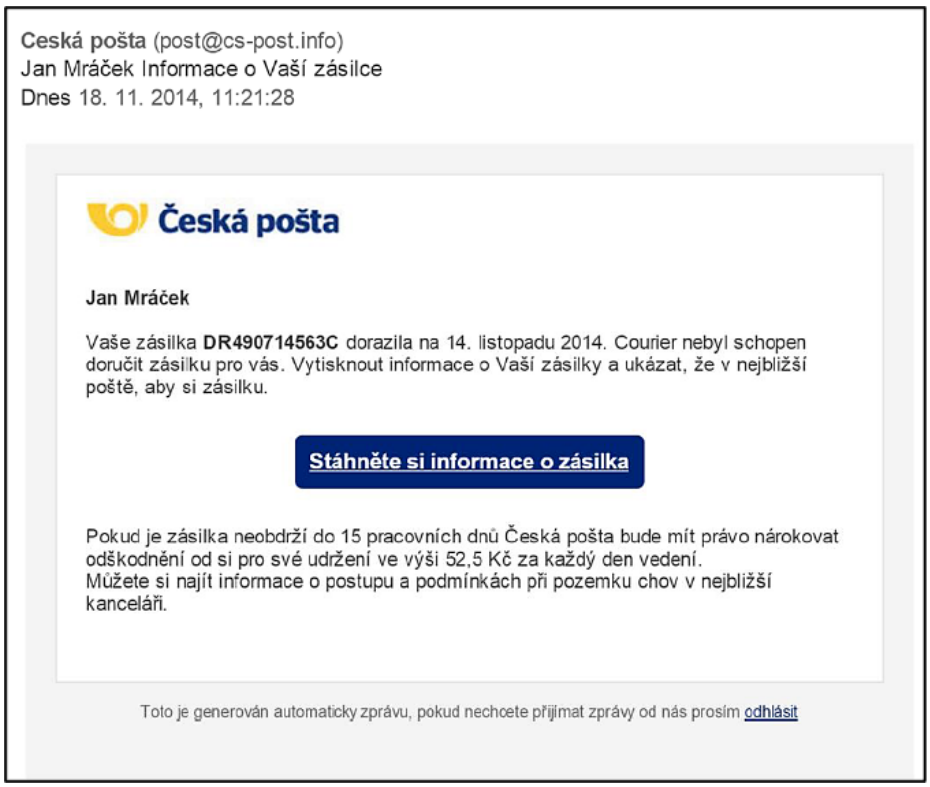
Dalším krokem útočníka pak již bylo odčerpání finančních prostředků z účtu napadeného na účet bílých koní, kteří měli následně hotovost vybrat či přeposlat na účty jiné. Díky plnému ovládání (pomocí malware) jak přístupových údajů do internetového bankovnictví (viz napadený počítač), tak ovládání druhotného autentizačního prostředku (viz napadený mobilní telefon – kdy autentizační zprávy byly přeposílány útočníkovi bez toho, že by se zobrazily oběti), mohl útočník zadat „legitimní“ příkaz k převodu peněz.

Dle zprávy společnosti Avast! za tímto útokem stáli rusky mluvící útočníci. SMS zprávy z infikovaného telefonu jsou přeposílány na číslo 79023501934, které je registrováno v oblasti Astrachaň, Rusko.[16]

4.6.1.2. Česká pošta

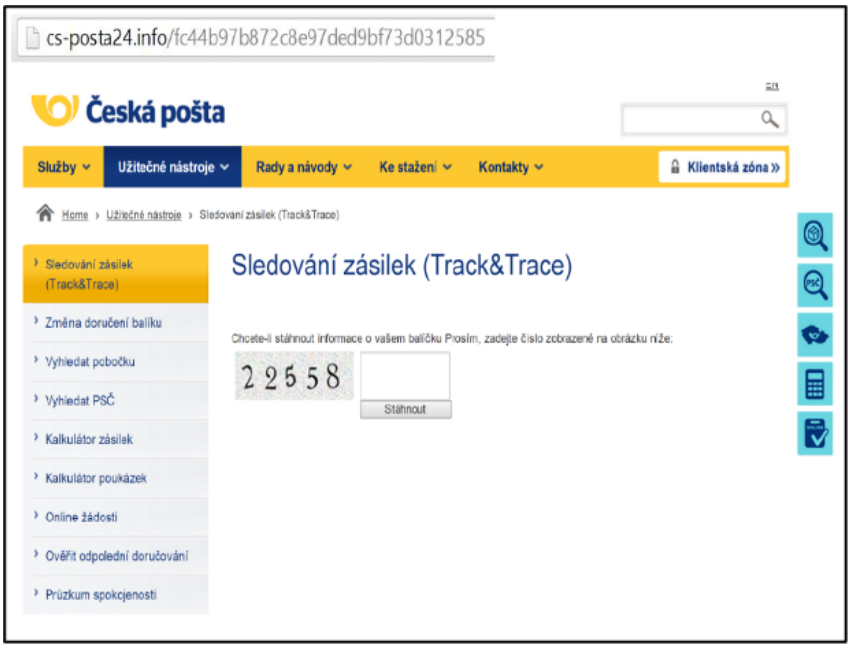
Druhý velký phishingový útok začal v listopadu 2014 a pokračoval až do prosince 2014. Na počátku útoku byl phishingový e-mail s oznámením „České pošty“ o tom, že jste nebyl jakožto adresát zásilky zastižen a že si máte stáhnout informace o zásilce. Čeština použitá v tomto phishingovém e-mailu je jednou z nejhorších, na kterou je možné u phishingu narazit. Ke generování tohoto e-mailu byl zřejmě použit některý z automatických překladačů z Internetu.

Podvodné e-maily byly rozesílány z adres, které nepatří české poště. Jednalo se například o asdresy: upport@cs-post.net, tracktrace@cs-post.net, cpost@cs-post.net, post@cs-post.net, zasilka@cs-post.net , které díky doméně ***cs-post*** mohly v uživateli vzbudit přesvědčení, že se jedná o stránky české pošty. Je třeba si však uvědomit, že ***cs-post*** byla zaregistrována v doméně ***.net***, kdežto skutečné stránky České pošty jsou zaregistrovány v doméně ***.cz*** (viz https://www.ceskaposta.cz).



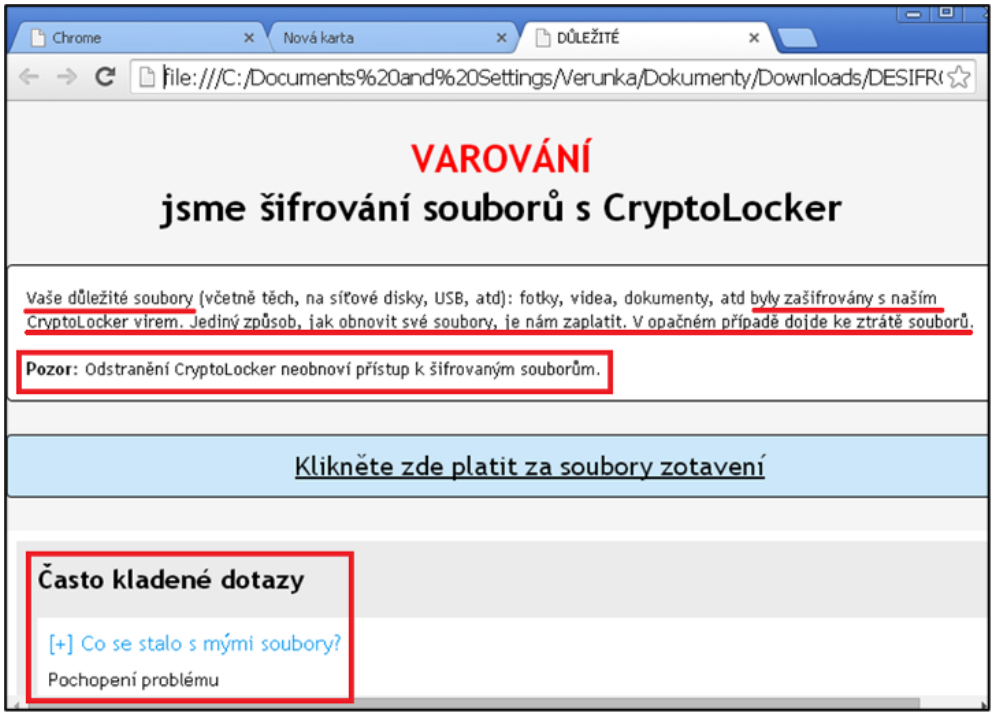
Obrázek 64 - Podvodný e-mail od "České pošty"

Pokud uživatel klikl na políčko: *Stáhněte si informace o zásilka*, byl přesměrován na stránky, které svojí vizáží připomínaly skutečné stránky České pošty. Zde byl uživatel vyzván k vepsání bezpečnostního kódu (Captcha) a následně mu bylo umožněno stáhnout soubor .zip, který obsahoval „informace o sledované zásilce“. Stejně jako v předchozí phishingové kampani byl v příloze uložen spustitelný soubor (ransomware), jehož cílem však bylo zašifrovat uživatelova data.



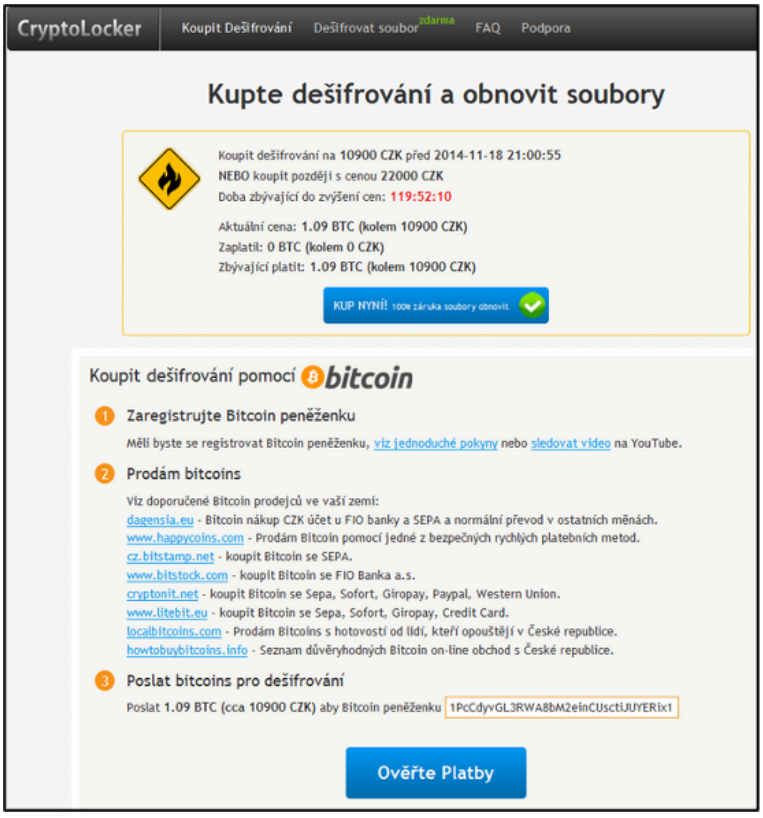
Podvodná stránka "České pošty"

Po zašifrování dat byla uživateli zobrazena výzva žádající zaplacení finanční částky za doručení klíče, který je schopen zašifrované soubory odšifrovat. Vlastní výzva již byla psána podstatně lepší verzí češtiny. Uživatel se také mohl dozvědět odpovědi na některé otázky, které ho případně trápily.



Informace, která se zobrazila uživateli po zašifrování jeho dat

Obnovení dat v té době stálo 1,09 BTC a uživateli byl kromě přepočtu na české koruny zobrazen i podrobný návod, jak si zřídit bitcoinovou peněženku, kde a jak nakoupit bitcoiny a kam je poslat.



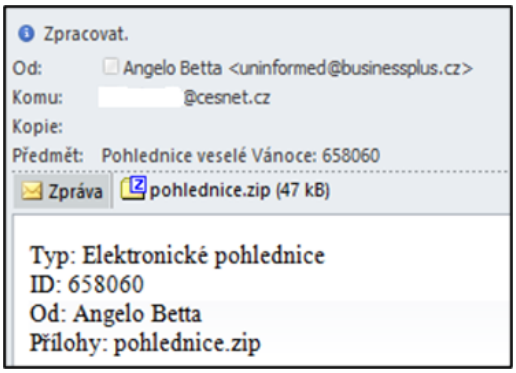
Návod na to, jak dešifrovat svoje soubory[17]

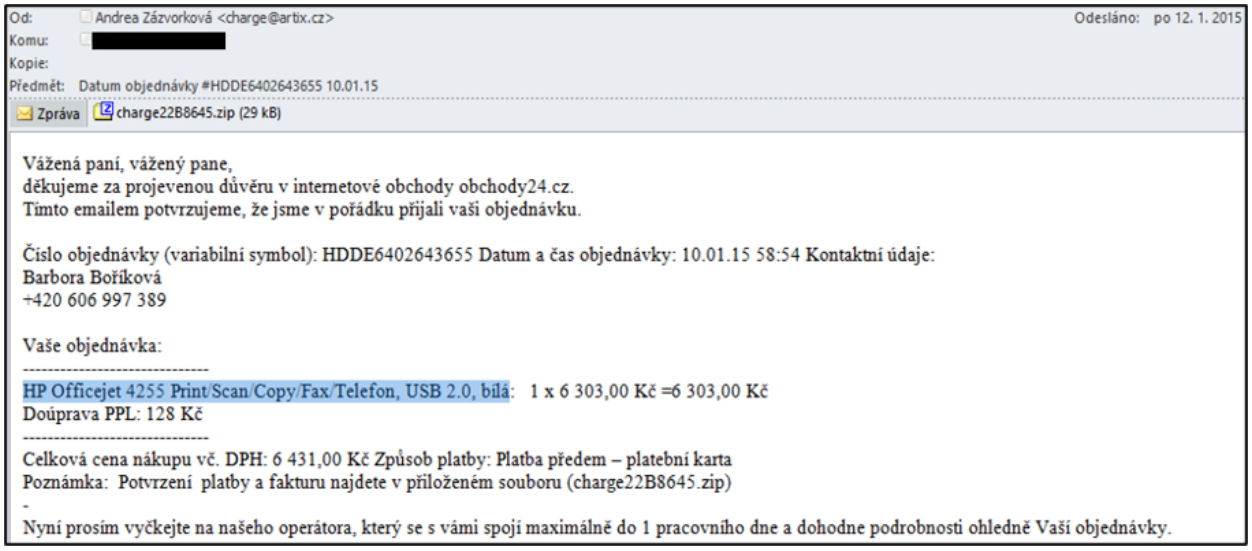
Vlastní útok je specifický tím, že jednak k phishingové kampani připojil ransomware, který rovnou začal zašifrovávat uživatelova data, a jednak tím, že k realizaci vlastního útoku bylo využito předvánoční období, ve kterém řada lidí čeká na doručení zásilek. Díky těmto dvěma faktorům byl vlastní útok velmi úspěšný.

4.6.1.3. Vánoce a dárky

Další velký phishingový útok začal v průběhu prosince 2014 (konkrétně v období vánoc) a pokračoval v lednu 2015. Tento útok byl rozdělen do dvou fází. V první fázi byly uživatelům zaslány e-mailové zprávy s přáním veselých Vánoc prostřednictvím elektronické pohlednice. V druhé fázi byly v průběhu ledna zasílány zprávy o potvrzení objednávky na elektroniku. Zpráva uživateli sdělila, že si zakoupil zboží (např. tiskárnu, harddisk, fotoaparát atp.), za které zaplatil předem platební kartou, přičemž odkazuje na fakturu v příloze.

Oba dva útoky mají společný prvek, kterým je malware obsažený v příloze e-mailu. Konkrétně se jednalo o Trojského koně (*Kryptik*), který byl prezentován jako spořič obrazovky. Tento malware byl stejně jako v případě útoku uvedeného v kap. 4.6.1.1 Dluh/Banka/Exekuce komprimován v souboru .zip. Po rozbalení souboru .zip nepovažovala řada uživatelů soubor *.scr*[18] za spustitelný program a infikovala si tak počítač.





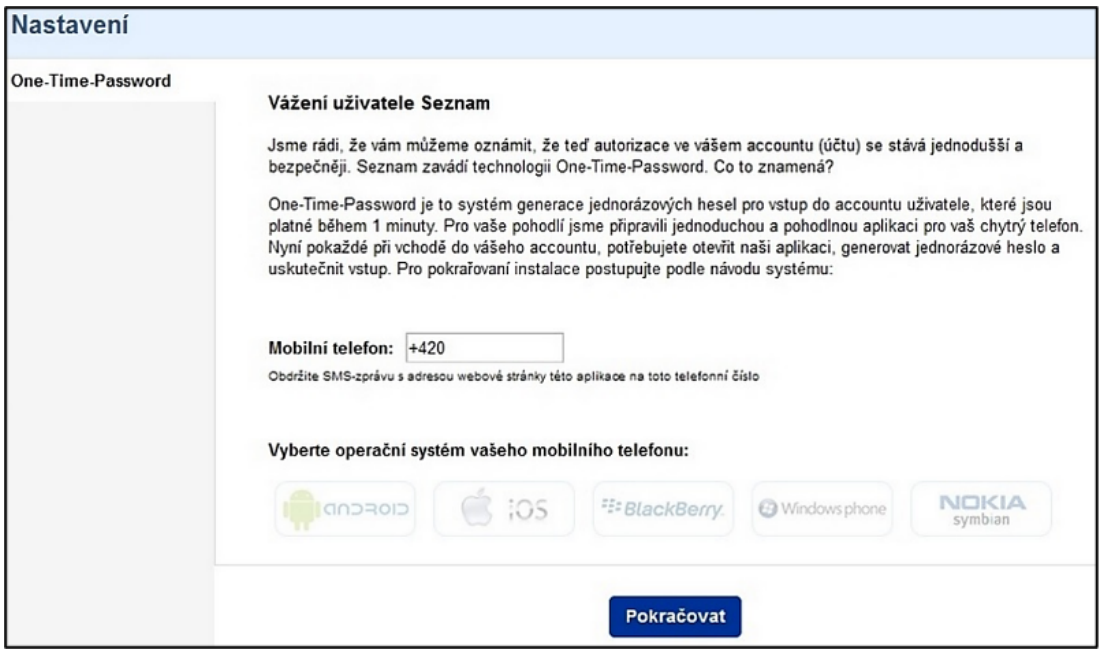
Ukázky phishingových zpráv pohlednice a obchod

Vlastní útok je specifický tím, že jednak využil typ souboru, který celá řada uživatelů nepovažuje za nebezpečný, a jednak načasováním útoku. Díky různým řetězovým e-mailům si uživatelé zvykli otevírat elektronické pohlednice či přílohy, které tak vypadají, bez důkladnějšího testování obsahu. Druhý útok byl naplánován tak, aby si uživatel prověřil, zda si skutečně neobjednal nějaké zboží, které mu díky vánočním svátkům nebylo doručeno.

4.6.1.4. Seznam.cz – One Time Password

Poslední phishingový útok demonstruje výraznou změnu v taktice útočníků. Útočník stále využívá té skutečnosti, že došlo k infikování počítače malwarem. Útočník může mít nad tímto počítačem sám kontrolu nebo si jej může pronajmout např. v rámci botnetu. K vlastnímu infikování mohlo dojít například pomocí jiného doručeného e-mailu, při návštěvě infikovaných stránek nebo jinak. Cílem útočníka v případě Seznam – One Time Password[19] bylo získat kontrolu nad mobilním telefonem uživatele.

Malware, který byl nainstalován v počítači, vyzval uživatele při přihlášení do e-mailové schránky Seznam.cz, aby si do svého mobilního telefonu nainstalovali prostředek pro jednodušší a bezpečnější práci se svou poštovní schránkou. Uživatel je následně krok za krokem proveden instalací aplikace SeznamOTP z nedůvěryhodného zdroje. Na konci instalace je uživateli poskytnut jeho „unikátní licenční klíč“. Ve skutečnosti si však uživatel nainstaloval do svého mobilního telefonu malware.



Úvodní obrazovka instalace SeznamOTP[20]

Riziko tohoto posledního phishingového útoku **spočívá v tom, že „phishingová zpráva" nebyla doručena prostřednictvím e-mailu nebo jiného komunikačního prostředku, ale byla zobrazena uživateli pouze při konkrétní situaci** (v tomto případě po přihlášení se do schránky seznam.cz) **a iniciátorem této zprávy byl malware nacházející se v již infikovaném počítači. Druhým rizikovým faktorem je ta skutečnost, že žádost o nastavení zabezpečení není nijak spojena s bankovním účtem. Uživatel si tedy nemusí uvědomit nebezpečí vyplývající z instalace této aplikace.**

V ČR je možné jednání, které má povahu „klasického phishingu", postihnout dle **§ 209** (Podvod) TZK. Podvod je dokonán obohacením se. Vytvoření repliky webové stránky a získání přihlašovacích jmen a vstupních hesel by pak bylo možné kvalifikovat jako přípravu či pokus trestného činu § 209 TZK. Samotné získání přístupových údajů, včetně čísel účtů, čísel platebních karet a PIN kódů bez jejich dalšího užití pak nebude trestné.

Možnosti trestněprávního postihu v ČR

V případě kombinovaných forem phishingových útoků, kdy je užit malware k infikování počítače, je třeba takovéto jednání pachatele postihnout také dle **§ 230** (Neoprávněný přístup k počítačovému systému a nosiči informací) TZK. Pokud je cílem phishingového útoku získat sobě nebo jinému neoprávněný prospěch, je možné uplatnit i ustanovení **§ 230 odst. 3** TZK.

Ve specifických případech by bylo možné využít i ustanovení **§ 234** (Neoprávněné opatření, padělání a pozměnění platebního prostředku) TZK.

4.6.2. Pharming

Pharming[21] představuje sofistikovanější a nebezpečnější formu phishingu. Jedná se o útok na DNS (Domain Name System) server, na kterém dochází k překladu doménového jména na IP adresu. K útoku dochází v momentě, kdy uživatel zadá na internetovém prohlížeči adresu webového serveru, na kterou chce přistoupit. Nedojde však k propojení na příslušnou IP adresu originálního webového serveru, ale na IP adresu jinou, podvrženou. Webové stránky na falešné adrese zpravidla velmi věrně imitují originální stránky, de facto jsou od nich k nerozeznání. Uživatel následně zadá přihlašovací údaje, které získá útočník. Tento útok je zpravidla realizován při přístupu uživatele na stránky internetového bankovnictví.

„Falešné webové stránky mohou sloužit k instalaci virů nebo trojských koní do uživatelova počítače nebo se pomocí nich mohou útočníci pokusit získat osobní či finanční údaje, které mohou být následně zneužity ke krádeži identity. Pharming je zvlášť nebezpečná forma kyberkriminality, protože v případě nakaženého serveru DNS se může uživatel stát obětí i v případě, že v jeho počítači není nainstalován vůbec žádný malware. Dokonce ani pokud používáte preventivní opatření, například zadáváte internetové adresy ručně nebo používáte výhradně důvěryhodné záložky, nejste před útokem tohoto druhu chráněni, protože k nechtěnému přesměrování dochází až poté, co počítač odešle žádost o spojení." ***[22]***

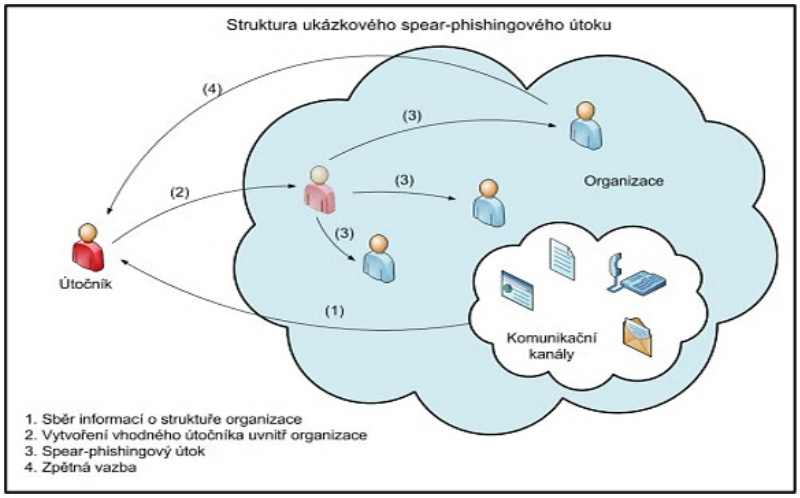
Druhým typickým způsobem pharmingu je napadení počítače koncového uživatele pomocí malware, kde se dá předpokládat menší míra zabezpečení. Tento malware změní soubor hostitelů s cílem odklonit přenos od zamýšleného cíle a přesměrovat uživatele na falešnou webovou stránku.

Trestněprávní postih je obdobný jako v případě phishingu.

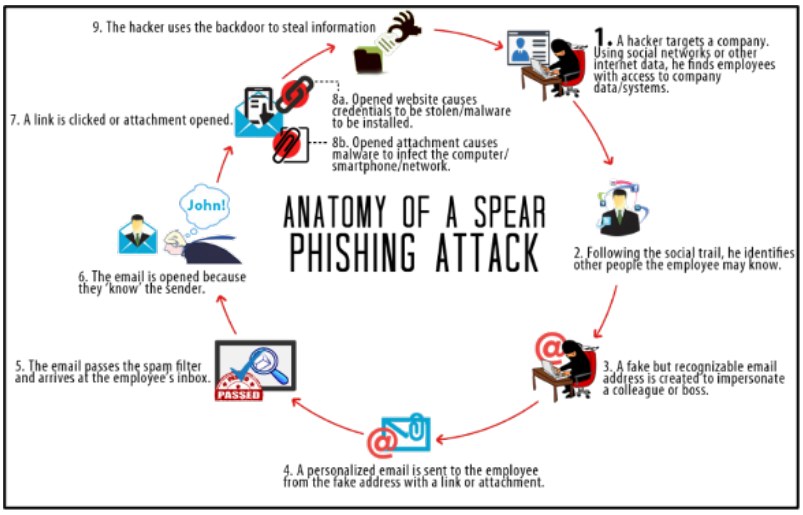
4.6.3. Spear Phishing

Spear phishing je jednou z forem phishingového útoku, avšak s tím rozdílem, že spear phishing je přesně cílený útok, na rozdíl od phishingu, který je útokem spíše plošným (nahodilým). Cílem útoku bývá konkrétní skupina, organizace nebo jednotlivec, konkrétně informace a data, která se v této organizaci nacházejí (např. duševního vlastnictví, osobní a finanční údaje, obchodní strategie, utajované informace aj.).

U spear phishingu oproti klasickému phishingu je rozdíl v tom, kdo je odesílatelem předmětných zpráv. V počátku útoku je to vlastní útočník, který využije otevřené zdroje, aby zjistil co nejvíce informací o napadané organizaci, její struktuře atd. Dále vytvoří velmi kvalitní e-mail či jinou zprávu a začne komunikovat s osobou zevnitř organizace jako s kolegou. Tuto osobu pak útočník využije jako prostředek pro šíření dalších zpráv (např. infikovaných malware) v rámci organizace. Jelikož se jedná o osobu obětem „známou", nemají problém s ní komunikovat a méně, pokud vůbec, prověřují její zprávy.[23]



Struktura Spear-Phishignového útoku[24]



Průběh spear phishingového útoku[25]

Možnosti trestněprávního postihu v ČR

Postih spear phishera je obdobný jako v případě phishingu. Za útokem typu spear phishing může být například i teroristická organizace. V tomto případě pak není vyloučena odpovědnost pro trestný čin dle **§ 311** (Teroristický útok) TZK.

4.6.4. Vishing

Pojem vishing[26] označuje telefonický phishing, při kterém útočník využívá technik sociálního inženýrství a snaží se od uživatele vylákat citlivé informace (např. čísla účtů, přihlašovací údaje – jméno a heslo, čísla platebních karet, aj). Útočník se záměrně snaží zfalšovat svoji identitu. Útočníci se často představují jako zástupci skutečných bank či jiných institucí, aby u uživatele vyvolali co nejmenší podezření. Vishing se používá ve VoIP (Voice over Internet Protocol) telefonii.

4.6.5. Smishing

Smishing[27] funguje na podobném principu jako vishing či phishing, ale k distribuci zpráv využívá SMS zprávy. V rámci smishingu jde primárně o snahu donutit uživatele zaplatit částku (například zavolat na placenou linku, poslat dárcovskou SMS aj.) nebo kliknout na podezřelé URL odkazy. Pokud uživatel uvedené URL navštíví, je přesměrován na stránku, která zneužívá určité zranitelnosti počítačového systému, případně je uživatel vyzván k zadání citlivých údajů či k instalaci malware.[28]

Příklad smishingu:

„Upozorneni – toto je automaticky vygenerovana zprava z (název lokální banky), Vase kreditni karta byla zablokovana. K reaktivaci volejte 866### ###“

Možnosti trestněprávního postihu v ČR

Trestněprávní postih vishingu i smishingu je obdobný jako v případě phishingu.

[1] Viz např. *Google says the best phishing scams have a 45-percent success rate.* [online]. [cit. 14.8.2016]. Dostupné z: https://www.engadget.com/2014/11/08/google-says-the-best-phishing-scams-have-a-45-percent-success-r/

Phishing by the Numbers: Must-Know Phishing Statistics 2016. [online]. [cit. 14.8.2016]. Dostupné z: https://blog.barkly.com/phishing-statistics-2016

[2] Viz např. *Beware of Fake Android Prisma Apps Running Phishing, Malware Scam* [online]. [cit.14.8.2016]. Dostupné z: https://www.hackread.com/fake-android-prisma-app-phishing-malware/

[3] LANCE, James. *Phishing bez záhad*. Praha: Grada Publishing, 2007. s. 45.

[4] **WILSON Tracy, V.** *How Phishing Works.* [online]. [cit.14.8.2016]. Dostupné z: http://computer.howstuffworks.com/phishing.htm

[5] LANCE, James. *Phishing bez záhad*. Praha: Grada, 2007, s. 35.

K problematice phishing dále srov. *Digital Doom's Digi World*, 2008. ISSN 1802-047X. [online]. [cit.14.8.2016]. Dostupné z: http://www.ddworld.cz/software/windows/jak-se-krade-pomoci-internetu-phishing-v-praxi.html

[6] K vývojovým trendům phishingu srov blíže např. DODGE, Ronald. C., Curtis CARVE a Aaron J. FERGUSON. Phishing for User Security Awareness. *Computers & Security*, 2007, roč. 26, č. 1, s. 73 – 80.

[7] **Dle následující studie vzrostl phishing o 250% za posledních 6 měsíců.** Viz *Phishing Activity Tresnds Report.* [online]. [cit.14.8.2016]. Dostupné z: https://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf

[8] Dále jen zkráceně **DBE**.

[9] Blíže viz např. *Uhraďte dluhy, toto je exekuční příkaz. Komora varuje před další vlnou podvodných e-mailů* [online]. [cit.15.8.2016]. Dostupné z: http://zpravy.aktualne.cz/finance/falesne-exekuce-jsou-zpet-komora-varuje-pred-dalsi-vlnou-pod/r~cbdac6de765111e599c80025900fea04/

[10] Blíže viz výsledky z Virustotal. [online]. [cit. 15.8.2016]. Dostupné z:

https://www.virustotal.com/cs/file/62170532b1f656c6917fa66d0ed98462e106f3aa139273c9f2c3a370a67d265f/analysis/1471330723/

[11] Computer Security Incident Response Team. Blíže viz např. https://www.csirt.cz/

[12] Viz např. *Pozor na zprávu o údajné neuhrazené pohledávce - jedná se o podvod.* [online]. [cit.15.8.2016]. Dostupné z: https://www.csirt.cz/page/2073/pozor-na-zpravu-o-udajne-neuhrazene-pohledavce---jedna-se-o-podvod/
Znovu se objevily podvodné zprávy. [online]. [cit.15.8.2016]. Dostupné z: https://www.csirt.cz/news/security/?page=97

PODVODNÉ EMAILY hrozí exekucí, nic neplaťte a neotvírejte! [online]. [cit.15.8.2016]. Dostupné z:

http://tn.nova.cz/clanek/zpravy/cernakronika/podvodne-emaily-hrozi-exekuci-nic-jim-neplatte-a-neotvirejte.html

Pozor na zprávu o výzvě k úhradě před exekucí - jedná se o podvod. [online]. [cit.15.8.2016]. Dostupné z: https://www.csirt.cz/news/security/?page=87

Čo sa skrýva v prílohe podvodných e-mailov? [online]. [cit.15.8.2016]. Dostupné z: https://blog.nic.cz/2014/07/23/co-sa-skryva-v-prilohe-podvodnych-e-mailov-2/

[13] Blíže viz rozbor funkčnosti malware Tinba: *W32. Tinba (Tinybanker)*. [online]. [cit.15.8.2016]. Dostupné z: https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_w32-tinba-tinybanker.pdf

[14] HOŘEJŠÍ, Jaromír. *Falešný exekuční příkaz ohrožuje uživatele českých bank.* [online]. [cit.15.8.2016]. Dostupné z: https://blog.avast.com/cs/2014/07/17/falesny-exekucni-prikaz-ohrozuje-uzivatele-ceskych-bank-2/

[15] Tamtéž – obrázek s captcha kódem.

[16] HOŘEJŠÍ, Jaromír. *Falešný exekuční příkaz ohrožuje uživatele českých bank.* [online]. [cit.15.8.2016]. Dostupné z: https://blog.avast.com/cs/2014/07/17/falesny-exekucni-prikaz-ohrozuje-uzivatele-ceskych-bank-2/

[17] *Sledování zásilky České pošty aneb nová havěť.* [online]. [cit.14.8.2016]. Dostupné z: http://www.viry.cz/sledovani-zasilky-ceske-posty-aneb-nova-havet/

[18] Soubory s příponou SCR jsou Spustitelné soubory.

Primárně je jim přiřazen program Unknown Apple II File (found on Golden Orchard Apple II CD Rom). Dále bývají přiřazovány také Windows Screen Saver, Image Pro Plus Ver. 1.x - 4.5.1.x Macro (Media Cybernetics Inc.), TrialDirector Script File (inData Corporation), Screen Dump, Screen Font, Statistica Scrollsheet, Procomm Plus Screen Snapshot File, Movie Master Screenplay, Mastercam Dialog Script File (CNC Software Inc.), Sun Raster Graphic, LocoScript Screen Font File (LocoScript Software), Faxview Fax, DOS DEBUG Input File, Script a FileViewPro.

Co znamená přípona souboru SCR. [online]. [cit.14.8.2016]. Dostupné z: http://www.solvusoft.com/cs/file-extensions/file-extension-scr/

[19] Dále jen **SeznamOTP**

[20] Další informace o tomto malware a průběhu celého útoku je možné nalézt např. na: *Podvodníci mění taktiku. Našli novou cestu, jak vybílit lidem účty.* [online]. [cit.14.8.2016]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/364094-podvodnici-meni-taktiku-nasli-novou-cestu-jak-vybilit-lidem-ucty.html

[21] Jedná se o kombinaci slov **farming** (farmaření/hospodaření) a **phreaking**.

[22] Blíže viz *Co je pharming?* [online]. [cit.14.8.2016]. Dostupné z: http://www.kaspersky.com/cz/internet-security-center/definitions/pharming

[23] *„Útočník si vyhlédne organizaci pracující s cennými informacemi, analýzou webových stránek získá informace o personální struktuře, zaměstnancích a procedurách (pro získání podrobnějších informací o zaměstnancích může využít jejich soukromé stránky a diskusní fóra) a v dalším kroku útočník vytvoří zprávu, jejíž obsah, forma a vzhled napodobuje vnitřní komunikaci v organizaci. Ve zprávě požádá zaměstnance o zadání citlivých informací pro přístup do počítačové sítě.“*

Evoluční teorie v podání spear phishingu. [online]. [cit.15.2.2010]. Dostupné z: http://connect.zive.cz/content/evolucni-teorie-v-podani-spear-phishingu

[24] Tamtéž

[25] *Tip of the month July 2016 – Avoid getting hooked by Phishing*. [online]. [cit.14.8.2016]. Dostupné z: http://www.intermanager.org/cybersail/tip-of-the-month-july-2016-avoid-getting-hooked-by-phishing/

[26] Jedná se o kombinaci slov voice (hlas) a phishing.

[27] Jedná se o kombinaci slov SMS a phishing.

[28] Např. **Xshqi** - *Android Worm on Chinese Valentine's day.* [online]. [cit.14.8.2016]. Dostupné z: https://securelist.com/blog/virus-watch/65459/android-worm-on-chinese-valentines-day/

Selfmite - *Android SMS worm Selfmite returns, more aggressive than ever.* [online]. [cit.14.8.2016]. Dostupné z: http://www.pcworld.com/article/2824672/android-sms-worm-selfmite-returns-more-aggressive-than-ever.html

4.7. Business Email Compromise (BEC)

Business Email Compromise[1] is a type of scam attack where an attacker impersonates an executive (typically the CEO), and attempts to get an employee, customer, or vendor to transfer money or sensitive information to the attacker.

The BEC scam could be linked to other forms of fraud like a romance, lottery, employment, and rental scams.

By the definition of FBI the BEC is *a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.* ***[2]***

Unlike a traditional phishing attack, BEC is targeted at a certain individual or organization. In the case of BEC, the attacker prepares for the attack very thoroughly and tries to obtain maximum information about the victim before the attack takes place. Usually they use websites, annual reports, information about the organization´s employees from social networks, from compromised email accounts, etc.

This high level of targeting helps these email scams to slip through spam filters and evade email whitelisting campaigns. It can also make it much, much harder for employees to recognize the email is not legitimate.[3]

The victims of the BEC scam range from small businesses to large corporations. The BEC scam is linked to other forms of fraud, including but not limited to: romance, lottery, employment, and rental scams.

The FBI warned that BEC scams would likely *„continue to grow, evolve, and target businesses of all sizes."* The FBI also mentioned that they've seen a 1,300% increase in business email compromise attacks since January 2015.[4]

The BEC attackers rely heavily on social engineering tactics to trick unsuspecting employees and executives. Some of the sample email messages have subjects containing words such as ***request***, ***payment***, ***transfer***, and ***urgent***, among others.

The BEC scam usually takes one of the following forms:

1. CEO Fraud

Attackers pose as the company CEO or other company executive and send a spoofed email to employees with the ability to send wire transfers, and instruct them to send funds to the attackers.

2. Fake Invoice[5]

A business, which often has a long standing relationship with a supplier, is requested to wire funds for invoice payment to an alternate, fraudulent account. The attacker typically approaches the victim via e-mail or telephone. An e-mail attack has typically a spoofed email source code (header) and subject of the request so it appears very similar to a legitimate request.

3. Account Compromise

This attack is similar to Fake Invoice. The attacker uses an employee's email account (hacked or spoofed), then sends an email to customers to announce them there has been a problem with their payment and they need to re-send it to a different account.

4. Business Executive and Attorney Impersonation

Victims are contacted by attackers, who identify themselves as lawyers or representatives of law firms. The attacker requests a large funds transfer to help settle a legal dispute or pay an overdue bill. The attacker is trying to convince victims that the transfer is confidential and time-sensitive, so it is less likely that the employee will attempt to confirm whether they should transfer the funds.

5. Data Theft

A type of BEC whose goal is not a direct money transfer. Typical victims of that attack include finance or HR departments /employees. The attacker is requests them to send highly sensitive to his account. The social engineering is used and the data theft attack can be a starting point to the above mentioned BEC attacks focused on financial transfer.

Since 2017, there has been a dramatic increase in fraudulent attacks having the character of BEC in the Czech Republic. Yet again, most BEC attacks use similar modus operandi:

1. Picking a victim and obtaining information about the victim (medium-sized and small organizations are the most common target)

2. Preparation of a spoofed email (to create a spoofed email, publicly available free services are used very often, e.g.: **www.5ymail.com**. This service allows the attacker to create and send any spoofed email which corresponds to an existing email. However, this service does not make it possible to receive answers and therefore it is necessary to redirect the email communication to another existing email, registered e.g. with a freemail service. The real identity can be found from the message source code.)

3. Sending a spoofed email to an employee of the victim (the most frequent BEC attacks include CEO Fraud and Fake Invoice. Sums required in this way usually range from several hundred euros to € 4000.)

4. Request for an immediate or "urgent" transfer of money to an account of the attacker or money mules [validation of the payment, as well as of the person who gives the command to make the payment, is the key moment when the completion of the criminal act can be prevented. If the organization has appropriately set up security protocols, such transfer usually does not take place. From the point of view of identification of the

attacker, the attacker´s account, or the account of money mules, is the tool which makes it possible to determine in practice whether it is the case of continuation of a criminal act (i.e. from the point of view of substantive criminal law one criminal act) or whether it is a case of concurrence of criminal acts. At the same time, it is de facto the most significant digital footprint which allows identification of the attacker.]

5. Money transfer to an account of the attacker or money mules

---

[1] BEC scams are also known as „CEO fraud" or „Man-in-the-Email" scams.

[2] *Business E-mail Compromise: The 3.1 Billion Dollar Scam*. [online]. [quote12.6.2018]. Available at: https://www.ic3.gov/media/2016/160614.aspx
[3] *What is a Business Email Compromise (BEC) Attack? And How Can I Stop It?* [online]. [quote12.6.2018]. Available at: https://blog.barkly.com/what-is-a-business-email-compromise-bec-attack-and-how-can-i-stop-it

[4] *Business E-mail Compromise: The 3.1 Billion Dollar Scam*. [online]. [quote12.6.2018]. Available at: https://www.ic3.gov/media/2016/160614.aspx

[5] This attack is also called: "The Bogus Invoice Scheme," "The Supplier Swindle," and "Invoice Modification Scheme."

4.8. Podvodné webové stránky (firmy)

Na Internetu se lze setkat s celou řadou aktivit, respektive webových stránek[1] prezentujících úžasné výhry či nabízejících různé zboží za velmi výhodné ceny. Útočníci využívají sociálního inženýrství a spoléhají primárně na důvěřivost a neopatrnost lidí. Vlastní činnost útočníka pak může mít typicky dvojí podobu.

V prvním případě se útočník snaží vylákat citlivé údaje (např. jméno, příjmení, doručovací adresa, e-mail, telefonní číslo a heslo) typicky za účelem registrace, doručení zboží, výhry aj. Všechny tyto údaje zadává uživatel sám a dobrovolně. Útočník se tak dostává k údajům, které může, stejně jako v případě phishingu, využít k celé řadě aktivit. Například na základě zadaného hesla a dalších údajů o uživateli se útočník může pokusit získat přístup k dalším službám, které uživatel používá.[2]

V druhém, mnohem častějším případě se pak jedná o aktivity, které spočívají v podvodném vylákání finančních prostředků z uživatele. Běžně jsou na Internetu nabízeny za velmi výhodnou cenu automobily, motocykly, traktory, další zemědělská technika a především elektronika jakéhokoliv druhu.

V souvislosti s podvodnými nabídkami na Internetu vydalo Evropské spotřebitelské centrum[3] doporučení pro uživatele, které by jim mělo umožnit poznat podvodná jednání:

· ***Zadejte údaje o společnosti (např. název společnosti, adresu webu, e-mail) do internetového vyhledávače.***

· ***Zamyslete se nad tím, jak se obchodník prezentuje.*** *Je vzhled webu, na kterém se chystáte nakoupit, profesionální? Důvěryhodný dojem rozhodně nebudí e-mailové adresy na bezplatných a anonymních serverech typu yahoo.com, hotmail.com, gmail.com, live.com, seznam.cz apod. Stejně tak, je-li web umístěn na bezplatném hostingovém serveru, není to znak profesionality.*

· ***Platbu předem provádějte jen tehdy, jde-li o skutečně důvěryhodného obchodníka.*** *Jistě nedáte peníze na ulici neznámému člověku s příslibem, že Vám v budoucnu dodá věc. Na internetu tak však řada uživatelů činí. Platbu předem provádějte jen tehdy, pokud jste si jisti, že jednáte s důvěryhodným dodavatelem. Především údaje o platební kartě je třeba chránit.*

· ***Zvlášť podezřelý je požadavek na platbu systémem Western Union.*** *U bankovních převodů nikdy nezasílejte peníze na účty soukromých osob, pokud se nejedná o účet prodávající firmy/společnosti.*

· ***Mezi obvyklé znaky podvodu patří špatná jazyková úprava, požadavek platby předem v hotovosti či převodem, další požadavky na platby pod smyšlenou záminkou*** *(clo, pojištění, přibalení většího počtu kusů výrobku)* ***a tak podobně. Pamatujte si, že pokud se nabídka zdá příliš výhodná, než aby byla skutečná, tak nejspíš skutečná není!***

· ***Nahlédněte do obchodního rejstříku dané země****, zda je v něm společnost registrována. (Stává se také, že někdo zneužije jméno existující společnosti a založí web s podobným označením.*

· ***Zkontrolujte doménu webové stránky.*** *Stává se, že webová adresa je stejná jako adresa skutečně existující a registrované firmy. Je zde ovšem jeden rozdíl - doména, tedy koncovka internetové adresy, je jiná (např. nikoli „.co.uk" pro Velkou Británii, ale třeba „.co.cc" pro Kokosové ostrovy).*

· ***Najděte si sídlo společnosti na internetovém serveru nabízejícím pouliční fotografie měst****, a to podle adresy, uváděné u inzerátů a na webové stránce společnosti.*

· ***Važte si svých osobních údajů.*** *Nesdělujte informace o sobě na nedůvěryhodných či Vám dosud neznámých stránkách. Uvádějte jen takové údaje, které jsou skutečně nezbytné.*

· ***Nereagujte na nevyžádanou poštu (spam).*** *Na nevyžádanou poštu nereagujte, v žádném případě nesdělujte e-mailem údaje o bankovním účtu, číslo platební karty nebo třeba přihlašovací údaje do internetového bankovnictví. Nevyžádaný e-mail smažte, nikdy neotvírejte neznámé přílohy.*[4]

Všechny výše uvedené znaky je třeba pokládat za pouhé indicie, které mohou vést k odhalení podvodu. Útočník může své jednání modifikovat na základě úspěšnosti vlastního útoku. **Mimo uvedených rad je vhodné využít i varování zveřejňované na dalších stránkách, například** www.podvodnefirmy.cz **aj.**

Možnosti trestněprávního postihu v ČR

V ČR je možné výše popsané jednání jednání postihnout dle **§ 209** (Podvod) TZK. Podvod je dokonán obohacením se. Vytvoření repliky webové stránky a získání přihlašovacích jmen a vstupních hesel by pak bylo možné kvalifikovat jako přípravu či pokus trestného činu § 209 TZK. Pokud by se útočník pokusil (§ 21 TZK) na základě získaných přístupových údajů o neoprávněný přístup do jiného účtu uživatele, mohlo by být takovéto jednání kvalifikováno i jako **§ 230** (Neoprávněný přístup k počítačovému systému a nosiči informací) TZK.

---

[1] Nejběžněji se jedná o webové stránky, inzertní portály, ale může se jednat i o účty na sociálních sítích aj.

[2] Velmi často dochází k zadávání stejného, nebo obdobného hesla ze strany uživatelů v rámci různých služeb online. Díky tomu může útočník využít např. techniku slovníkového útoku k prolomení přístupových údajů k dalším službám. Tímto jednáním se útočník může dopustit i dalších protiprávních jednání (např. viz kap. 4.15 Identity theft, 4.8 Hacking aj.).

Blíže viz např. *Slovníkový útok.* [online]. [cit.30.8.2016]. Dostupné z: https://managementmania.com/cs/slovnikovy-utok

[3] Blíže viz http://www.evropskyspotrebitel.cz/

[4] Blíže viz *ESC radí, jak poznat podvody na internetu.* [online]. [cit.30.8.2016]. Dostupné z: http://www.evropskyspotrebitel.cz/nakupy-online/esc-radi-jak-poznat-podvod-na-internetu-27250

4.9. Hacking

Pojem hacking je v současné době veřejností vnímán pejorativně jako jakákoliv činnost osoby směřující k získání nelegálního přístupu k cizímu systému či osobnímu počítači.[1] Zejména ve sdělovacích prostředcích bývají tímto pojmem všeobecně nazýváni všichni útočníci, jejichž jednání směřuje proti informačním technologiím či jejichž činnost je na využívání těchto technologií založena.[2] V tomto kontextu je však zásadní rozdíl mezi vnímáním obsahu pojmu hacking z pohledu veřejnosti, a z pohledu osob, které se samy za hackery označují nebo jsou za ně označovány vlastní komunitou.

Pojem **„hacker“**[3] a „**hacking**“ pochází z USA, vznikl v 50. letech 20. století a **označoval technicky nadanou osobu** (a její činnost) **schopnou nalézat nová, mnohdy neortodoxní řešení problému.**

Pro pochopení, jak vnímají společnost a její pravidla útočníci, jež jsme si zvykli označovat jako hackery, je vhodné poznat jejich názor. V roce 1984 Levy definoval následující principy hackerské etiky:

1. Přístup k počítačům a čemukoliv dalšímu, co tě může naučit něco o tom, jak svět funguje, by měl být neomezený a absolutní. Vždy respektuj pravidlo osobní zkušenosti.
2. Veškeré informace by měly být bezplatné.
3. Nevěř autoritám, podporuj decentralizaci.
4. Hackeři by měli být souzeni podle svých činů a nikoliv podle scestných kritérií jako jsou věk, rasa či postavení.
5. Na počítači můžeš vytvářet „krásu“.
6. Počítače mohou změnit tvůj život k lepšímu.[4]

Byť tato pravidla nejsou vždy respektována či uznávána, představují základní rámce vnímání virtuálního světa útočníky, jež označujeme za hackery.

Dalším významným vhledem do vnímání světa očima hackera je dokument Hackerův manifest:

Následující text byl napsán krátce po mém zatčení...

Svědomí hackera

Dneska chytli dalšího. Jsou toho plný noviny. "Mladík odsouzen za Skandální Počítačový Zločin", "Hacker zatčen za průnik do banky"...

Zasraný děti. Všechny jsou stejný.

Ale zkusili jste se někdy s tou svou trojitou psychologií a technomozkem padesátejch let podívat očima hackera? Položili jste si někdy otázku, jaká síla ho zformovala, co vytvářelo jeho osobnost?

Jsem Hacker. Vstup do mého světa...

Můj život začíná školou... Jsem chytřejší něž většina ostatních děcek, ty kecy, co nám vykládají, mě nudí...

Zasranej flákač. Všichni jsou stejný.

Jsem na gymplu nebo na střední. Učitelka už popatnáctý vysvětluje, jak se krátí zlomek. Chápu to. "Ne, slečno Smithová, nepsal jsem postup. Udělal jsem to z hlavy..."

Zasraný děcko. Nejspíš to někde opsal. Všichni jsou stejný.

Dneska jsem udělal objev. Objevil jsem počítač. Počkej chvíli, to je skvělý. Dělá to, co chci. A když to udělá chybu, tak je to kvůli tomu, že jsem něco zvoral. A ne jenom proto, že mě nemá rád...

...nebo se cítí být mnou ohrožený...

...nebo si myslí, že jsem vychcanej parchant...

...nebo že nemám rád učení a neměl bych tu bejt...

Zasraný děcko. Furt jenom hraje samý hry. Všechny jsou stejný.

A pak se to stalo... otevřely se dveře do světa... elektronický signál se řítí telefonní linkou jako heroin žilou narkomana, nachází úkryt před ubíjející každodenností... nachází board.

"To je to místo... sem patřím..."

Každýho tu znám. I když jsem je v životě neviděl, nikdy jsem s nima nemluvil, a možná že už o nich nikdy neuslyším... Znám vás všechny...

Zatracený děti. Furt jenom obsazujou linku. Všechny jsou stejný...

Vsaď prdel, že jsme všichni stejný!

Ve škole jste nás krmili po lžičkách dětským jídlem a my chtěli steak... kusy masa, který k nám proklouzly, byly předžvýkaný a bez chuti. Ovládali nás sadisti a ignorovali tupci. Bylo pár těch, co nás mělo učit a našlo v nás ochotné žáky, ale těch bylo jako kapek vody v poušti.

*"**Toto je teď náš svět...** Svět elektronů a spínačů, krása baudu. **Využíváme existujících služeb bez placení, mohly by být skoro zadarmo, kdyby nepatřily šmelinářským hltounům, a vy nás nazýváte zločinci. My objevujeme... a vy nás nazýváte zločinci. Dychtíme po vědomostech... a vy nás nazýváte zločinci. Existujeme bez barvy pleti, bez národnosti, bez náboženských předsudků a vy nás nazýváte zločinci. Vy stavíte atomové bomby, vy vedete války, vy vraždíte, podvádíte a lžete nám a chcete, abysme věřili tomu, že je to pro naše vlastní dobro, přesto jsme my zločinci.***

Ano, jsem zločinec. Mým zločinem je zvědavost. Mým zločinem je posuzování lidí podle toho, co říkají a co si myslí, a ne podle toho, jak vypadají. Můj zločin je to, že jsem chytřejší než ty, což je věc, kterou mi nikdy neodpustíš. Jsem Hacker a toto je můj manifest. Můžete zastavit jednotlivce, ale nemůžete nás zastavit všechny... konec konců, všichni jsme stejní.

Mentor

Hackerův manifest[5]

8. ledna 1986

V současné době sami hackeři užívají označení hacker pro osoby, které mají vynikající znalosti fungování informačních a komunikačních systémů, počítačových systémů, jejich operačních systémů a dalších programů, jejich síťových principů a mechanismů, přičemž jsou zároveň i vynikajícími programátory schopnými tvořit vlastní software, a to ve velmi krátkém čase. Právě snaha o poznání, jakým způsobem informační technologie, aplikace či technický prostředek fungují, a zpřístupnění těchto informací i ostatním uživatelům, je hnacím motorem i filozofií řady osob. Schopnost hackera získávat si díky vlastním navrženým a napsaným počítačovým programům přístup do počítačových systémů i mimo běžné způsoby přístupu (což ovšem nutně neznamená, že zisk takového přístupu musí být motivován snahou způsobit uživateli škodu, jinou újmu nebo se na proniknutí do systému jinak obohatit), je jednou, nikoliv jedinou dovedností.

Rozdělení hackerů

Právě motivace získání nestandardního (nikoliv nutně nelegálního) přístupu, způsob provedení takového průniku, jejich motivace a případné nakládání se získanými daty jsou klíčovými faktorem pro rozlišení těchto osob do následujících tří základních skupin:[6]

White Hats – jsou to hackeři, kteří uskutečňují své průniky do systému za využití bezpečnostních slabin systému právě za účelem odhalení těchto bezpečnostních mezer a vytvoření takových mechanismů a bariér, které by tyto útoky měly znemožňovat. Jsou často zaměstnanci či externími spolupracovníky renomovaných společností podnikajících v oblasti informačních technologií. Svým průnikem do systému nezpůsobují uživatelům škodu či jinou újmu, naopak v mnoha případech upozorňují správce takto napadeného systému na bezpečnostní chyby. Jejich činnost je zásadně nedestruktivního charakteru.

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

Gray Hats – jde o šedou zónu hackerů, tedy o osoby, které se nevyprofilovaly směrem k uvedeným dvěma skupinám. Občas z jejich strany může dojít k porušení práva jiného nebo morálních principů, avšak jejich činnost není primárně hnána snahou o způsobení škody, jako tomu je u Black Hats.

Kromě výše uvedeného, tj. nejběžněji používaného dělení, je možné hackery dělit do dalších skupin na základě jejich motivu. Jedná se o: Script Kiddies, Hactivists, státem sponzorované hackery, Spy hackers, kyber teroristy, začátečníky (n00b), Blue Hat hackers aj.[7]

Klíčovým faktorem pro posouzení hackingu jakožto možné bezpečnostní hrozby je stanovení důvodu aktivit hackera (viz rozdělení hackerů). V některých případech pak hacking může představovat reálnou bezpečnostní hrozbu, neboť se jedná o narušení bezpečnosti počítačového systému, případně prolomení ochrany či využití slabin systému. Naopak v jiných případech může být vhodným doplňkem sloužícím ke zvýšení bezpečnosti systému jako celku či nalezení slabých míst a zranitelností.

V obecné rovině je možné skutečně za hacking označit jakýkoliv neoprávněný průnik do počítačového systému z vnějšku, nejčastěji v rámci sítě Internet. Avšak ne každý hackerský útok musí být nutně označován za delikt.

Nebezpečí hackerských aktivit spočívá mimo jiné i v tom, že vedle vlastního získání neoprávněného přístupu do napadeného systému (bez ohledu na motivaci hackera) tyto osoby k realizaci těchto útoků vytvářejí a užívají vysoce efektivní softwarové prostředky, jejichž zdrojové kódy jsou hackery samotnými často následně zveřejněny např. v rámci Darknetích tržišť. To může vést k dalšímu hromadnému zneužívání těchto programů uživateli, kteří sami neovládají programování na takové úrovni, aby tyto programy vytvořili, avšak díky existenci takto zpřístupněných nástrojů mohou potenciálně způsobovat uživatelům napadených systémů poměrně značné škody. Prostřednictvím Internetu je tak možné si obstarat často celé sady hackerských softwarových programů obsahující základní software a informace nutné k jeho použití, de facto bez hlubších znalostí fungování těchto programů.

Formy hackingu

Vlastní činnost hackerů spočívá v celé řadě jednání. Mezi typické aktivity používané hackery patří:

1. Sociální inženýrství
2. Prolamování hesel[8]
3. Skenování portů[9]
4. Využívání malware k infiltraci počítačového systému
5. Phishing

6. Cros Site Script[10]

7. Odposlech komunikace[11]

Známé hackerské skupiny a hackeři

Asi nejznámější současnou hackerskou skupinou je Anonymous, avšak existují či existovaly další skupiny:[12]

- Anonymous
- Lizard Squad
- The Level Seven Screw
- Chaos Computer Club
- Lulzsec
- Syrian Electronic Army
- Globalhell
- Network Crack Program Hacker Group
- Antisec Movement
- Legion of Doom (1984-2000)
- Masters of Deception (1989-1993)
- Milw0rm aj.

Mezi **nejznámější hackery** patří Johnatan James, Vladimir Levin, Gary McKinnon, John McAfee, Astra, Stephen Wozniak, James Kosta, Kevin Mitnick, Adrian Lamo, David L. Smith.[13]

Není pochyb o tom, že **ne každá aktivita hackerů je legální**. Ve vztahu k zásahu do počítačového systému jistě dojde k porušení zaručených základních lidských práv a svobod.

Možnosti trestněprávního postihu v ČR

Jak bylo uvedeno výše, existuje celá řada jednání či útoků, které je možné podřadit pod pojem hacking (prolomením hesla počínaje a konče komplikovaným phishingovým útokem, který je kombinován se sociálním inženýrstvím a užitím malware).

Jednání hackera, spočívající pouze ve využití svých schopností, díky nimž překoná bezpečnostní opatření a získá přístup k počítačovému systému nebo jeho části, je možné postihnout dle **§ 230 odst. 1** (Neoprávněný přístup k počítačovému systému a nosiči informací) TZK.

V případě kombinovaných forem útoků, kdy je například užit malware k infikování počítače, je třeba takovéto jednání pachatele postihnout také dle **§ 230 odst. 2** (Neoprávněný přístup k počítačovému systému a nosiči informací) TZK. Pokud je cílem útoku získat sobě nebo jinému neoprávněný prospěch, nebo neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat, je možné uplatnit i ustanovení **§ 230 odst. 3** TZK.

[1] Blíže srov. např. GRIFFITHS, Mark. Computer Crime and Hacking: a Serious Issue for the Police? *The Police Journal,* 2000, roč. 73, č. 1, s. 18 –24.

YAR, Majid. Computer Hacking: Just Another Case of Juvenile Delinquency? *The Howard Journal*, 2005, roč. 44, č. 4, s. 387 – 399.

[2] Srov. např. články v denním tisku:

Největší hackerský útok potvrzen. V ohrožení jsou stovky miliónů uživatelů. [online]. [cit.16.8.2015]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/405260-nejvetsi-hackersky-utok-potvrzen-v-ohrozeni-jsou-stovky-milionu-uzivatelu.html

Hackeři se vydávají za Anonymous a hrozí útokem českým firmám. [online]. [cit.16.8.2015]. Dostupné z: http://www.lupa.cz/clanky/hackeri-vydavajici-se-za-anonymous-hrozi-utokem-na-ceske-firmy-chteji-zaplatit/

Yahoo řeší, jestli má hacker opravdu údaje o 200 milionech účtů. [online]. [cit.16.8.2015]. Dostupné z: http://www.lupa.cz/clanky/yahoo-resi-jestli-hacker-opravdu-ma-udaje-o-200-milionech-tamnich-uctu/

Hackeři zaútočili na uživatele Facebooku. [online]. [cit.16.8.2015]. Dostupné z: http://tech.ihned.cz/c1-37133210-hackeri-zautocili-na-uzivatele-facebooku-chteli-jejich-hesla

Hackeři ukradli Američanům data o novém typu bojových stíhaček. [online]. [cit.16.8.2015]. Dostupné z:

http://digiweb.ihned.cz/c1-36816420-hackeri-ukradli-americanum-data-o-novem-typu-bojovych-stihacek

Hackeři vám už brzy ukradnou data přímo z klávesnice. [online]. [cit.16.8.2015]. Dostupné z:

http://digiweb.ihned.cz/c1-29295240-hackeri-vam-brzy-ukradnou-data-primo-z-klavesnice

[3] Tento pojem lze přeložit mnoha způsoby a je třeba vycházet z kontextu. V americkém žargonu to původně znamenalo bezcílně se projíždět na koni. Hack také označoval jednoduché řešení problému. Následně znamenalo spáchání nějaké nepravosti studenty univerzity.

[4] LEVY, Steven. *Hackers: Heroes of the Computer Revolution* Sebastopol, CA: O'Reilly edia, s. 32-41. ISBN 978-1449388393.

Dostupné i online:

https://e11c1b148f6c7c56754c9184e0d1c52ac4d888f9-www.googledrive.com/host/0ByAMXZI2-PZ0WjBPYmhaWVVRN0E

[5] Český překlad převzat z: *1986 – Hackerův manifest.* [online]. [cit.16.8.2015]. Dostupné z: http://blisty.cz/art/14662.html

Originální znění je možné nalézt Phrack.org. [online]. [cit.16.8.2015]. Dostupné z: http://phrack.org/issues/7/3.html

[6] Označení těchto skupin, jakkoliv bizardní, je v informačních sférách reálně užíváno a nebývá překládáno do českého jazyka.

[7] Blíže viz např. SHNEIER, Bruce. *The Seven Types of Hackers.* [online]. [cit.16.8.2015]. Dostupné z: https://www.schneier.com/blog/archives/2011/02/the_seven_types.html

7 Types of Hacker Motivations. [online]. [cit.16.8.2015]. Dostupné z: https://blogs.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations/

7 Types of Hackers You Should Know. [online]. [cit.16.8.2015]. Dostupné z: https://www.cybrary.it/0p3n/types-of-hackers/

[8] Jde o proces získávání hesla k počítačovému systému. Běžně se k prolamování hesel používá:

§ Hádání hesla hrubou silou (testování hesla. Prevencí je dostatečně silné heslo);

§ Hádání hesla na základě určitých znalostí o uživateli (získaných například na sociálních sítích aj.);

§ Využití slovníku běžně používaných hesel (slovníkový útok);

§ Vyžádání hesla od administrátora systému vydáváním se za oprávněného uživatele (Útočník předstírá zapomenuté heslo a pokusí se jej obnovit.)

§ Odchytávání hesel z nešifrované nebo nedostatečně šifrované síťové komunikace mezi počítačovým systémem a uživatelem

§ Hledání hesel v souborech dat uložených systémem

[9] Jde o metodu, při níž jsou zjišťovány otevřené síťové porty na počítačovém systému, který je připojen k počítačové síti. Na základě tohoto zjištění je možné určit, jaké služby jsou na počítačovém systému spuštěny (např. webový server, ftp server aj.) Vlastní útok je pak zaměřen na zjištěné spuštěné služby na základě jejich zranitelností.

[10] Jedná se o útok spočívající v narušení webových stránek. Při tomto způsobu útoku je využito aktivních prvků (skriptů) na webové stránce, do kterých je vložen zákeřný kód a následně je nabídnut oběti.

Jedno z méně častých, avšak o to nebezpečnějších jednání spočívá ve zneužití zranitelnosti webové aplikace pro spuštění malware v rámci prohlížeče oběti. Oběť pak není schopna takové jednání odhalit. Závadný kód je spuštěn stejně jako zbytek stránky a útočníkovi je umožněno převzít oprávnění prohlížeče v rámci systému.

Blíže viz např. *OWASP, XSS* [online]. [cit.15.7.2016]. Dostupné z: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

[11] Viz kap. 4.11 Sniffing.

[12] Blíže viz např. *10 Most Notorious Hacking Groups.* [online]. [cit.15.7.2016]. Dostupné z: https://www.hackread.com/10-most-notorious-hacking-groups/

Obrázek převzat z [online]. [cit. 15.7.2016]. Dostupné z:

http://img02.deviantart.net/a2fd/i/2012/330/7/5/we_are_anonymous_by_mrj_5412-d5mb6xc.jpg

[13] Blíže viz např. *10 Most notorious hackers od all time.* [online]. [cit.15.7.2016]. Dostupné z: https://hacked.com/hackers/

Nejznámější počítačoví hackeři a jejich útoky. [online]. [cit.15.7.2016]. Dostupné z: https://www.stream.cz/top-5/10004402-nejznamejsi-pocitacovi-hackeri-a-jejich-utoky

4.10. Cracking

Pojem **cracking** je s pojmem hacking spojován, někdy jsou dokonce tyto pojmy veřejností či ve sdělovacích prostředcích nesprávně zaměňovány. Pojem lze do českého jazyka přeložit jako louskání či pukání. Obsahově pojem cracking znamená prolamování nebo obcházení ochranných prvků počítačového systému, programů nebo aplikací, s cílem jejich následného neoprávněného užití.

Za crackery bývají označováni hackeři z kategorie Black Hats, tedy ti, kteří uskutečňují průlomy do systémů ve snaze způsobit uživateli škodu, získat informace, popřípadě sebe nebo jiného obohatit. Dále je cracking spojen zejména s porušováním autorských práv a práv souvisejících s právem autorským. Za cracking je v tomto smyslu označováno jednání spočívající v obcházení ochranných prvků, které brání vytváření kopií či nelegálnímu užívání počítačových programů a hudebních nebo filmových produktů (filmová či hudební CD, DVD apod.). Tyto bezpečnostní prvky jsou využívány jako prostředky ochrany autorských práv ve smyslu § 43 odst. 1 AZ, ve znění pozdějších předpisů.

Jednou z forem cracingu je i **„password cracking“** sloužící ke zjišťování přístupového hesla do počítačového systému, licencovaného systému či programu. Pokud jde o porušování autorského práva, pak cracker zpravidla vytvoří keygen či crack[1], který umožní následné užití programu. Takto upravené programy jsou pak zpravidla sdíleny na warez fórech či P2P sítích.

Možnosti trestněprávního postihu v ČR

Jednání pachatele, v rámci kterého dochází k prolamování ochrany počítačového systému či programu, s úmyslem zisku informací a jejich následném neoprávněném užití naplňuje skutkovou podstatu trestného činu dle **§ 230 odst. 1 či 2** (Neoprávněný přístup k počítačovému systému a nosiči informací) TZK. Pokud je cílem crackingu získat sobě nebo jinému neoprávněný prospěch je možné uplatnit i ustanovení **§ 230 odst. 3** TZK

Vyloučena není ani trestněprávní odpovědnost dle **§ 231** (Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat) TZK. Při distribuci chráněného autorského díla pak dochází k naplnění **§ 270** (Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi) TZK.

---

[1] **Keygen** – Key Generator. Program generující sériová čísla, případně další údaje. **Crack** – program sloužící k odstranění, či omezení funkčnosti ochranných prvků jiného programu.

4.11. Internetové (počítačové) pirátství

Každý autor má právo stanovit, jak s jeho dílem můžete nakládat.

Nesouhlasím-li s podmínkami užití díla,

nerozumím jim nebo je neznám,

mám právo dílo neužívat.

Jan Kolouch

Pojem Internetové pirátství je pojmem obecným, zastřešujícím kriminalitu, jež porušuje práva duševního vlastnictví (velmi často zužovaná pouze na právo autorské). Teprve s rozšířením počítačových systémů a zejména nástupem Internetu se dá hovořit o masovém pirátství, jakožto jedné z nejrozšířenějších forem kybernetické trestné činnosti.

Porušování práv duševního vlastnictví, zejména autorských práv a práv souvisejících s právem autorským, patří v prostředí informačních technologií v současné době k jednomu z nejpalčivějších problémů.

4.11.1. Právo duševního vlastnictví

Ve vztahu k internetovému pirátství je třeba nejprve vymezit problematiku duševního vlastnictví, zejména pak práva autorského. Toto vymezení je nezbytné pro pochopení rozdílu mezi legálním a protiprávním jednání osob, které jsou na Internetu činné.

Právo duševního vlastnictví představuje majetek nehmotné povahy, tzv. „nehmotné statky", které jsou **výsledkem tvůrčí činnosti člověka.** Toto právo je **nezávislé na hmotném substrátu** (může být proto užíváno kdykoliv a kdekoliv na světě) za podmínky, že je **jedinečné, neopakovatelné a dostatečně originální.**

Právo duševního vlastnictví je možné rozdělit do dvou oblastí:

1) **Autorská práva** (chrání např. původní literární a umělecká díla, hudební skladby, televizní vysílání, počítačové programy, databáze, reklamní výtvory, multimédia aj.)

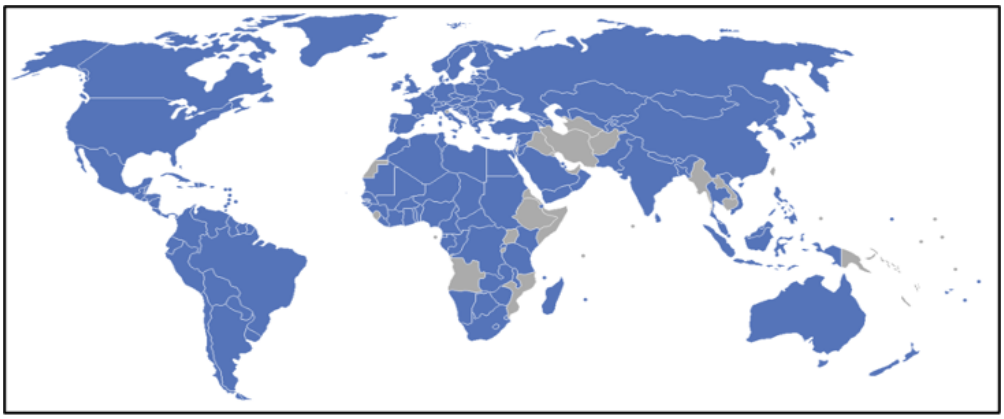
2) **Průmyslová práva** (chrání např. patenty na vynálezy, vzory, průmyslové modely, ochranné známky, zeměpisný původ aj.)

Z hlediska zaměření této monografie se dále budu primárně zabývat pouze právem autorským a zásahům do tohoto práva.

4.11.2. Legislativní rámec

Ochrana práv autorských začala být poprvé na mezinárodní úrovni řešena v 19. století, a mezi nejvýznamnější právní dokumenty, které se jí věnují, patří:

- **Bernská úmluva o ochraně literárních a uměleckých děl**[1] (1886), která byla následně doplňována a upravována [1908 (Berlín), 1928 (Řím), 1948 (Brusel), 1967 (Stockholm), 1971 (Paříž).]. Od roku 1967 se její správou zabývá **WIPO** *(World Intellectual Property Organization – Světová organizace duševního vlastnictví)*.



***Obrázek 73 - Seznam států. Modře jsou vyznačeny státy, které přijaly Bernskou úmluvu.*[2]**

- Dohoda o obchodních aspektech práv k duševnímu vlastnictví, která je jednou z příloh Dohody o zřízení Světové obchodní organizace (WTO) – viz sděl. č. 191/1995 Sb., (**TRIPS – Trade Related Aspects of Intellectual Property Rights**)[3]
- Mezinárodní úmluva o ochraně výkonných umělců, výrobců zvukových záznamů a rozhlasových organizací ze dne 26. října 1961 (vyhl. č. 192/1964 Sb., ve znění opravy č. 157/1965 Sb.) – **Římská úmluva**[4]
- Smlouva Světové organizace duševního vlastnictví o právu autorském Ženeva 1996 ze dne 20. prosince 1996 (viz sděl. 33/2002 Sb. m. s.), (**WCT – WIPO Copyright Treaty**)[5]
- Smlouva Světové organizace duševního vlastnictví o výkonech výkonných umělců a o zvukových záznamech Ženeva 1996 ze dne 20. prosince 1996

(viz sděl. 48 / 2002 Sb. m. s.), (**WPPT – WIPO Performances and Phonograms Treaty**)[6]
- Úmluva o ochraně výrobců zvukových záznamů proti nedovolenému rozmnožování jejich zvukových záznamů ze dne 29. října 1971 (viz vyhl. 32/1985 Sb.) – **Ženevská úmluva**[7]
- Všeobecná úmluva o autorském právu revidovaná v Paříži dne 24. července 1971 (viz vyhl. č. 134/1980 Sb.) [8]
- Směrnice Rady 91/250/EHS ze dne 14. května 1991 o právní ochraně počítačových programů,
- Směrnice Rady 92/100/EHS ze dne 19. listopadu 1992 o právu na pronájem a půjčování a o některých právech v oblasti duševního vlastnictví souvisejících s právem autorským, v platném znění,
- Směrnice Rady 93/83/EHS ze dne 27. září 1993 o koordinaci určitých předpisů týkajících se práva autorského a práv s ním souvisejících při družicovém vysílání a kabelovém přenosu,
- Směrnice Rady 93/98/EHS ze dne 29. října 1993 o harmonizaci doby ochrany práva autorského a určitých práv s ním souvisejících, v platném znění,
- Směrnice Evropského parlamentu a Rady 96/9/ES ze dne 11. března 1996 o právní ochraně databází,
- Směrnice Evropského parlamentu a Rady 2001/29/ES ze dne 22. května 2001 o harmonizaci určitých aspektů práva autorského a práv s ním souvisejících v informační společnosti,
- Směrnice Evropského parlamentu a Rady 2001/84/ES ze dne 27. září 2001 o právu na opětný prodej ve prospěch autora originálu uměleckého díla,
- Směrnice Evropského parlamentu a Rady 2004/48/ES ze dne 29. dubna 2004 o dodržování práv duševního vlastnictví.
- Úmluva Rady Evropy č. 185 o kyberkriminalitě.

4.11.3. Vlastní útoky

Pro fenomén porušování práv autorských a práv souvisejících s právem autorským se v prostředí Internetu vžilo několik pojmů. Nejčastěji bývá užíván pojem **softwarové pirátství** (pro porušování autorských práv ve vztahu k počítačovým programům) a **audiovizuální pirátství** (pro porušování autorských práv k audiovizuálním dílům – hudebním a filmovým). **Základem pro softwarové i audiovizuální pirátství je však vždy porušení některého z autorských práv či práv souvisejících s právem autorským**.[9] Obecným pojmem, který zastřešuje softwarové a audiovizuální pirátství, je pojem Internetové (někdy též počítačové) pirátství.

Trestné činy proti duševnímu vlastnictví se značně rozšířily právě s masovým nástupem Internetu. Jako nejběžnější případy porušování autorského díla v kyberprostoru lze uvést:

- *šíření díla elektronickou poštou*, což je nejjednodušší způsob k šíření malých souborů (zejména literárních či grafických autorských děl),

- *zveřejnění díla na webových stránkách* bez souhlasu autora. Jedná se o další velmi jednoduchý způsob porušování autorského práva. Zveřejňovány jsou menší soubory (z hlediska velikosti dat) a toto nelegální jednání je zpravidla velmi brzy odhaleno.

- *rozšiřování díla nahráním na specializovaný server*, odkud je možné volně dané dílo stáhnout (např. Megaupload, Rapidshare),

- *šířením díla za využití Peer-to-peer (P2P) sítí*. [10] Tyto sítě jsou schopné přenášet/sdílet obrovská množství dat (v řádech několika GB až desítek TB). V rámci nich dochází k nejzávažnějšímu porušování autorských práv.

- *zásahy do počítačových programů s cílem překonat technická opatření nositele autorských práv zabraňujících pořizování kopií takto chráněných programů* (tzv. crack),

- *rozšiřování díla pomocí datových nosičů přímo mezi uživateli* (půjčování a následné okopírování dat z DVD, HDD apod., prodej datových nosičů a další),

- *pořízení záznamu přímo při produkci a její následné rozšíření* (např. pořízení obrazového záznamu filmového díla přímo z plátna) – tzv. camcording,

- *neoprávněné projekce audiovizuálních děl*,

- *již vlastní obstarání si počítačového díla*. Počítačový program požívá zvláštní ochrany a není možné bez souhlasu nositelů autorských práv ve smyslu autorského zákona pořizovat rozmnoženiny takového díla, a to ani pro vlastní potřebu,

- *užívání počítačového programu v rozporu s licencí*,

- a další.

Mezi nejčastější projevy audiovizuálního pirátství patří zejména neoprávněné šíření audiovizuálních děl pomocí počítačových sítí, opatřování záznamu filmových děl přímo při promítání v kině a jejich následné „umístění" ke stažení v kyberprostoru, šíření originálních nosičů s filmovým či hudebním dílem v rozporu s licenčním ujednáním, výroba a šíření padělků originálních filmových či hudebních děl a veřejné projekce filmových děl v rozporu s licenčním ujednáním. Dále pak jednání spočívající v šíření softwarových produktů, zásazích do softwarových produktů, nelegální výroba softwarových produktů a užívání softwarových produktů v rozporu s licenčním ujednáním. Porušením autorského práva bude již vlastní neoprávněné obstarání softwarového produktu, aniž by s ním bylo dále nakládáno.

Umístění díla (bez ohledu na to, jestli audiovizuálního či softwarového) do kyberprostoru (**upload**) naplňuje znak šíření díla ve smyslu autorského zákona a (pokud není autorem nebo jinou oprávněnou osobou dovoleno) může být trestně postižitelné. **Neoprávněným užitím díla je též zveřejnění odkazu na místo v kyberprostoru, odkud je možné dílo získat.**

Pokud jde o srovnání se zahraniční právní úpravou, je vhodné se zmínit o francouzském zákonu HADOPI,[11] který měl chránit před internetovým pirátstvím. Dle tohoto zákona vznikl zvláštní úřad, jehož úkolem bylo zjišťovat ilegální stahování materiálu podléhajícího autorským právům. Ti uživatelé, kteří si stáhli hudbu a filmy z Internetu bez zaplacení (vyjma volně šiřitelných děl), byli třikrát varováni a při nerespektování těchto varování byl předmětný úřad oprávněn odpojit je od Internetu až na jeden rok.[12] Avšak ani takto přísný zákon neomezil počet nelegálního stahování autorských děl. Zároveň však nastolil řadu otázek týkající se přípustnosti zásahu do základních lidských práv a svobod bez rozhodnutí soudu.[13] Zákon HADOPI byl zrušen 10. července 2013.

V souvislosti s internetovým pirátstvím se často objevuje též pojem „Warez". **Warez představuje,** velmi zjednodušeně řečeno, **formu počítačového pirátství**, kde informační technologie jsou pouze prostředkem pro urychlení šíření nelegálních kopií autorských děl prostřednictvím Internetu. Warezová fóra v současnosti slouží zejména ke stahování cracků a keygenů, ale i kompletních upravených programů, filmů a hudby. Výsledný produkt warezové scény se nazývá **release**. Pro ochranu soukromí používají klienti warezových fór proxy servery a bouncery sloužící k maskování jejich IP adresy, a tím znemožňující případné sledovaní. Vlastní komunikace a nabízení release probíhá v privátních místnostech, vytvořených k tomuto účelu na Internetu, kam mají přístup pouze členové skupiny.

Možnosti trestněprávního postihu v ČR

Poskytování souborů, ať v rámci warezu či P2P sítě, lze postihnout dle **§ 270** (Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi), případně dle **§ 231** (Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat) TZK.

---

[1] Dostupná online. [online]. [cit.15.7.2016]. Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?page=0&idBiblio=34669&nr=133~2F1980&rpp=100#local-content; http://www.zakonyprolidi.cz/cs/1985-19

[2] *Bernská úmluva o ochraně literárních a uměleckých děl.* [online]. [cit.15.7.2016]. Dostupné z: https://cs.wikipedia.org/wiki/Bernsk%C3%A1_%C3%BAmluva_o_ochran%C4%9B_liter%C3%A1rn%C3%ADch_a_um%C4%9Bleck%C3%BDch_d%C4%9B. Předložená mapa je pouze ilustrační a nezobrazuje aktuální geopolitické členění světa. Kompletní seznam států, které ratifikovaly smlouvu WIPO, je možné nalézt na: http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=15

[3] Dostupná online. [online]. [cit.15.7.2016]. Dostupné z: http://www.mkcr.cz/assets/autorske-pravo/sb51-95.pdf

[4] Dostupná online. [online]. [cit.15.7.2016]. Dostupné z: http://www.zakonyprolidi.cz/cs/1964-192; http://www.zakonyprolidi.cz/cs/1965-157

[5] Dostupná online. [online]. [cit.15.7.2016]. Dostupné z: http://www.mkcr.cz/assets/autorske-pravo/sb015-02m.pdf

[6] Dostupná online. [online]. [cit.15.7.2016]. Dostupné z: https://www.mkcr.cz/assets/autorske-pravo/sb021-02m.pdf

[7] Dostupná online. [online]. [cit.15.7.2016]. Dostupné z: http://www.zakonyprolidi.cz/cs/1985-32

[8] Dostupná online. [online]. [cit.15.7.2016]. Dostupné z: http://www.zakonyprolidi.cz/cs/1980-134

[9] Blíže k této problematice srov. VOLEVECKÝ, Petr. Kybernetické trestné činy v trestním zákoníku. *Trestní právo*, 2010, roč. 14, č. 7 - 8, s. 34 a násl.

[10] Zapojením do P2P začíná uživatel, při standardním nastavení, automaticky sdílet s dalšími (jemu zpravidla neznámými) uživateli, svůj obsah. Typicky je při stahování (download) automaticky nastaveno i nabízení (upload) stahovaného materiálu.

[11] **HADOPI** (High Authority for Copyright Protection and Dissemination of Works on the Internet law), Fr: ***Loi favorisant la diffusion et la protection de la création sur Internet.***

[12] Úřad k tomuto rozhodnutí nepotřeboval rozhodnutí soudu. Na základě stanoviska Ústavního soudu Fr. z 22. listopadu 2009 je k odpojení vyžadován souhlas soudu.

[13] Blíže viz např. *Francie zakáže internetové pirátství.* [online]. [cit.15.7.2016]. Dostupné z: http://www.blisty.cz/2009/5/13/art46807.html

Přísný zákon proti hudebním a filmovým pirátům Francii nepomohl. [online]. [cit.15.7.2016]. Dostupné z: http://technet.idnes.cz/prisny-zakon-proti-hudebnim-a-filmovym-piratum-francii-nepomohl-phi-/sw_internet.asp?c=A100330_095705_sw_internet_vse

France drops controversial 'Hadopi law' after spending millions. [online]. [cit.15.7.2016]. Dostupné z: https://www.theguardian.com/technology/2013/jul/09/france-hadopi-law-anti-piracy aj.

4.12. Sniffing

Sniffing je metoda nelegálního odposlechu dat procházejících počítačovou sítí při komunikaci mezi poskytovanou službou a počítačovým systémem prostřednictvím tzv. **snifferu.**[1]

Technicky sniffing znamená odchytávání a čtení TCP paketů. Z bezpečnostního pohledu je sniffing možné označit také jako monitoring sítě, či monitoring provozu sítě a jedná se o jeden ze standardních prostředků pro diagnostiku sítě, respektive diagnostiku anomálií v síťovém provozu. Monitoring sítě je pak schopen zobrazit například nestandardní komunikaci počítačového systému napadeného malwarem atp. Vlastní činnost správců sítě v případě monitoringu sítě není nelegální (pokud se nedopustí dalšího jednání, které by mohlo případnou právní odpovědnost zakládat – např. instalace keylogger, či jiného malware do počítačového systému bez vědomí uživatele), neboť umožňuje udržet a spravovat počítačovou síť.

K monitoringu síťového provozu je využívána celá řada nástrojů (např. Wireshark[2], NetWorx, PRTG Network monitor aj.).

Pro to, aby bylo možné sniffing subsumovat pod jeden z projevů kyberkriminality, je třeba, aby osoba provádějící tuto činnost jednala nelegálně, typicky bez souhlasu či vědomí uživatele. Z dat zachycených sniffingem je útočník schopen extrahovat a složit citlivé informace o uživateli, např. přihlašovací údaje (uživatelské jméno a heslo), e-mailovou či VOIP komunikaci, informace o používaných službách aj. Ke sniffingu může být využit i malware v podobě trojských koní, keyloggerů nebo například spyware.

Password Sniffer Spy. Rozmazaná jsou jména a hesla. [3]

Možnosti trestněprávního postihu v ČR

De facto by takovou činnost bylo možné označit jako **nelegální odposlech a záznam telekomunikačního provozu**. Výše popsaným jednáním jistě dojde k zásahu do základních lidských práv a svobod, zejména se jedná o **čl. 13** Listiny, **a je zcela lhostejné, zda nelegální sniffing provádí externí útočník, či administrátor sítě.** Dle norem trestního práva by bylo možné takové jednání subsumovat pod **§ 182 odst. 1** (Porušení tajemství dopravovaných zpráv) TZK a v případě zneužití takto získaných informací by se mohlo jednat o trestný čin dle **§ 182 odst. 2** TZK. Pokud uvedenou nelegální činnost provádí zaměstnanec provozovatele poštovních služeb, telekomunikační služby nebo počítačového systému anebo kdokoli jiný vykonávající komunikační činnosti, mohl by naplnit znaky skutkové podstaty dle **§ 185 odst. 5** TZK.

---

[1] **Sniffing** je anglické slovo znamenající - **čmuchat, čenichat**. Sniffer je pak možné krkolomně přeložit jako čichač.

[2] Blíže k použití software Wireshark např. *How to use Wireshark to capture, Filter and inspect Packets.* [online]. [cit.15.7.2016]. Dostupné z: http://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/

MINAŘÍK, Pavel. *Wireshark – Paketová analýza pro všechny.* [online]. [cit.18.8.2016]. Dostupné z: https://www.systemonline.cz/it-security/wireshark-paketova-analyza-pro-vsechny.htm

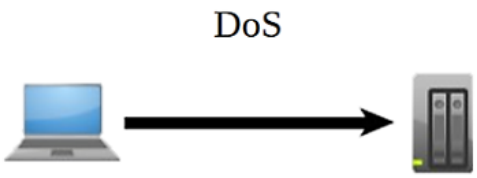
[3] *Password Sniffer Spy.* [online]. [cit.18.8.2016]. Dostupné z: http://securityxploded.com/password-sniffer-spy.php

4.13. DoS, DDoS, DRDoS útoky

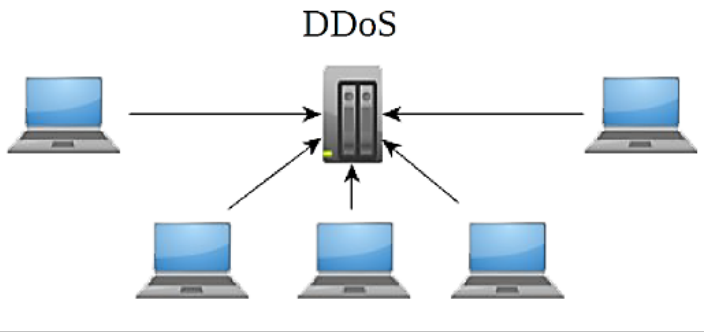
Pojem **DoS** je zkratkou z anglického spojení slov „***denial of service***“, což lze do českého jazyka přeložit jako „popření či odepření služby“. Jedná se o jednu z forem útoků na (internetovou) službu, jehož cílem je vyřazení z činnosti nebo snížení výkonu napadeného technického zařízení.[1] Tento útok je realizován zahlcením napadeného počítačového systému (či prvku sítě) pomocí opakujících se požadavků na úkony, které má počítačový systém vykonat. Tento útok může být realizován i zahlcením informačních kanálů mezi serverem a počítačem uživatele či zahlcením volných systémových prostředků. Systém napadený DoS útokem se projevuje zejména neobvyklým zpomalením služby, celkovou nebo chvilkovou nedostupností služby (např. webových stránek) apod.

Rozdíl mezi DoS, DDoS a DRDoS útoky spočívá především v tom, jakým způsobem je útok veden. Pro názornost jsou k jednotlivým typům útoku přiloženy obrázky demonstrující způsob provedeného útoku.

V případě **DoS (Denial of Service)** je zdroj útoku jeden. Tomuto typu útoku je relativně snadné se ubránit, neboť je možné blokovat provoz ze zdroje útoku.

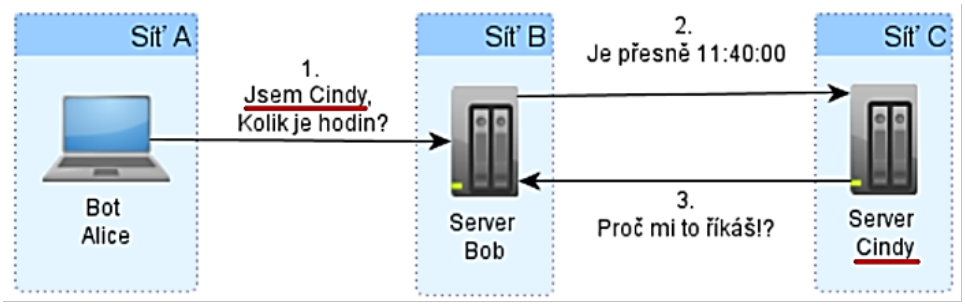


U **DDoS** (**Distributed Denial of Service** - distribuované odepření služby) dochází k zahlcení cílového počítačového systému **odesíláním paketů z více počítačových systémů, které jsou různě geograficky umístěny, což ztěžuje obranu a identifikaci útočníka.** Takové útoky byly užity např. proti Yahoo! Inc., elektronickým obchodům aj.[2] Velmi často jsou k tomuto typu útoků využívány botnety či aktivity uživatelů podporujících určitou online kampaň (viz dále – Anonymous a LOIC).



V případě **DRDoS** (**Distributed Reflected Denial of Service** – Distribuované, odražené popření služby) se jedná o podvržený distribuovaný DoS útok, který využívá mechanismus tzv. odražení. Útok spočívá v rozeslání podvržených požadavků na spojení na velké množství počítačových systémů, které poté na tyto požadavky odpoví, ovšem ne iniciátorovi spojení, ale oběti. Podvržené požadavky na spojení mají totiž jako zdrojovou adresu uvedenou adresu oběti, která je pak zahlcena odpověďmi na tyto požadavky. Řada počítačových systémů se tak stává nedobrovolným účastníkem útoku vlastně tím, že korektně odpoví na žádost o navázání spojení.

DoS, DDoS, DRDoS útoky velmi často využívají chyby například v operačním systému, spuštěných programech či síťových protokolech - UDP, TCP, IP, http aj.



Existuje několik základních metod DoS či DDoS útoku, přičemž mezi nejznámější patří:[3]

- Zahlcení příkazem ping (*Ping-Flood*)

Díky protokolu Internet Control Message Protokol a nástroje Ping (Packet Internet Groper) je možné příkazem „ping“ zjistit „živost“ počítačového systému s danou IP adresou a detekci času odezvy takového systému. V rámci útoku Ping-Flood dochází k zahlcení oběti velkým množstvím tzv. ICMP Echo Request paketů, na které oběť začne odpovídat - posílat tzv. ICMP Echo Replay pakety. Útočník doufá, že se tím oběti zahltí šířka pásma (pro příjem i odesílání dat). Vlastní útok je možné ještě zesílit tím, že se pingu emitujícímu ICMP pakety nastaví možnost flood (záplava). Dané pakety se poté začnou odesílat, aniž by čekaly na odpovědi. Pokud je cílový počítačový systém málo výkonný, je možné jej takto učinit nedostupným.

- Zahlcení volných systémových prostředků (*SYN-Flood*)

SYN-Flood je druh útoku, kdy se útočník snaží svoji oběť zahltit velkým množstvím žádostí o navázání spojení. Útočník pošle posloupnost paketů s příkazem SYN (tzv. SYN pakety) cílovému počítačovému systému (oběti), přičemž cílový systém na každý SYN paket odpoví zasláním SYN-ACK paketu, avšak útočník již dále neodpovídá. Cílový počítačový systém čeká na finální potvrzení, tzv. ACK paket od iniciátora spojení (útočníka) a drží pro toto spojení alokované zdroje, kterých má ale omezené množství. Tím může dojít k vyčerpání systémových zdrojů cíle útoku.[4]

- **Falšování zdrojové adresy** (*IP spoofing*)

IP Spoofing představuje aktivity spočívající v podvrhávání (falšování) zdrojové adresy odesílaných paketů, kdy útočník iniciující spojení ze stroje A s **IP dresou a.b.c.d** jako zdrojovou adresu do odesílaných paketů vloží např. **IP adresu d.c.b.a.** a odešle je cíli B. Cíl B pak odpovídá na tuto zdrojovou adresu, tzn. odpověď neadresuje na IP adresu a.b.c.d, ale adresuje ji na IP adresu **d.c.b.a.** Pomocí této metody lze zhoršovat (zesilovat) útoky typu DoS, DDoS. Útočník tuto techniku používá tehdy, když na svoji žádost o navázání spojení nepotřebuje od cíle odpověď, pouze jej chce zaměstnat. Když útočník jako zdrojovou IP adresu do odesílaných paketů uvede IP adresu cíle svého útoku (např. a.a.a.a) a pakety vyšle na mnoho jiných počítačových systémů (IP adres), tyto pak odpovídají počítačovému systému a.a.a.a. Tímto způsobem se realizuje útok typu DRDoS.

- **Smurf attack**

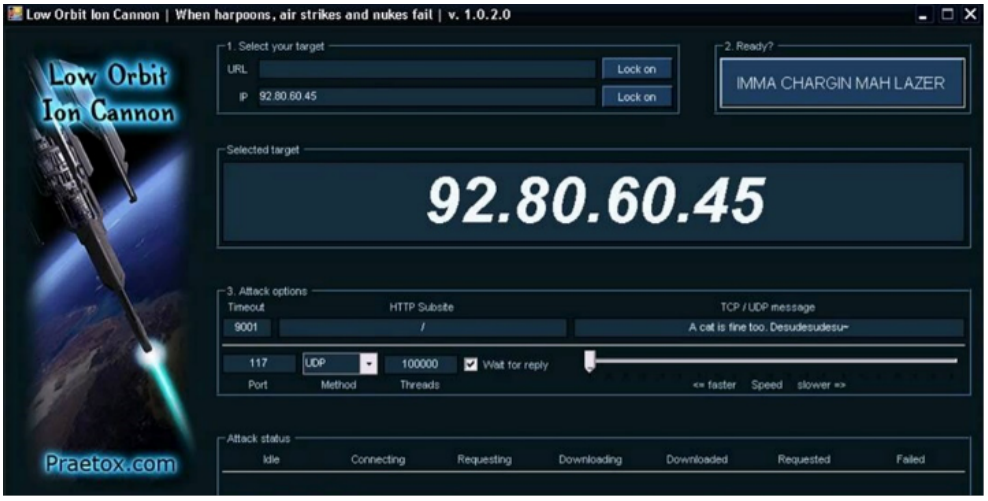
Tento útok je realizován prostřednictvím chybné konfigurace systému, který povolí rozesílání paketů všem počítačům zapojeným v počítačové síti skrze broadcast adresu.

Cílem útoků typu DoS/DDoS obvykle **není infikovat počítač**, respektive počítačový systém, **nebo překonat bezpečnostní ochranu např. heslem**, které jej chrání, ale pomocí série opakovaných požadavků **jej buď zahltit, či dočasně vyřadit z provozu**. Typicky tak dojde k omezení či zablokování přístupu ke službám.

Pro to, aby bylo možné „útočníka" DoS či DDoS útoků právně postihnout, je třeba určit, zda jeho **jednání bylo protiprávní,** a pokud ano, jak moc závažné toto jednání bylo. Jde o to, že povahu DDoS útoku může mít například i zcela korektní činnost uživatelů Internetu, kteří se v jeden okamžik (v krátkém časovém období) snaží připojit např. na webový server společnosti, která poskytuje slevy na letenky a kupř. oznámila, že od 12.00 hod dojde k plošnému snížení letenek o 75 %. Nebo může jít o přístup velkého množství uživatelů na webovou službu některého z populárních médií, které referují o významné nebo mediálně zajímavé události – nástupu nového prezidenta, úmrtí významné osobnosti apod. Pokud je cílový počítačový systém (webserver) nedostatečně dimenzován nebo je špatně nakonfigurován (není schopen odbavit požadovanou sumu přístupů), dojde k jeho „kolapsu" obdobně, jako tomu je u cíleného DDoS útoku. Je pak otázkou, zda by se měli postihovat uživatelé, kteří se na uvedený web snažili v daný čas přihlásit, a tím de facto způsobili odstavení předmětné služby.

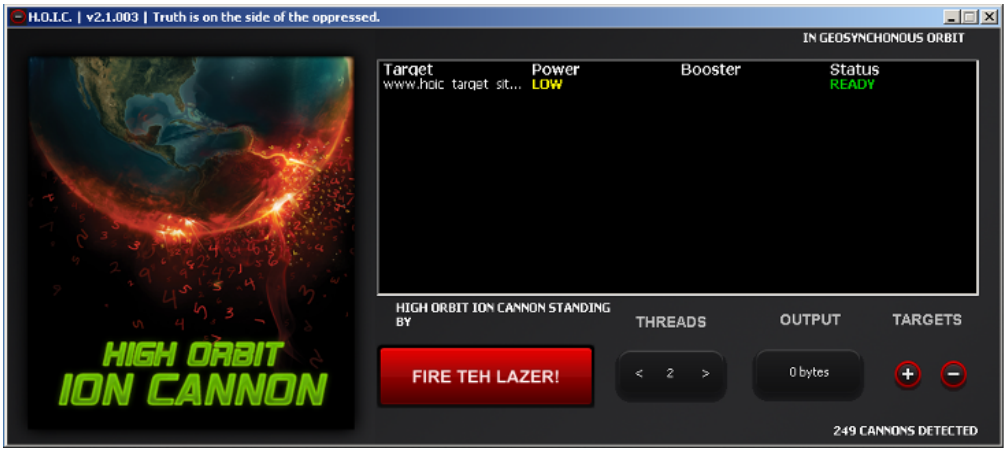
Domnívám se, že v nastíněných případech, byť uživatelé způsobili masivní DDoS útok na službu poskytovatele, není reálné, ba ani myslitelné, tyto „pseudoútočníky" postihnout jakýmikoli prostředky práva, neboť jejich jednání nebylo od počátku protiprávní.

Odlišným případem by však byla situace, kdy se útočníci např. prostřednictvím Internetu svolávají a v konkrétní čas, díky svému opětovnému přihlašování k poskytované službě, tuto službu potlačí.[5] K takovýmto případům docházelo např. v rámci protestů proti ACTA (Anti-Counterfeiting Trade Agreement) v roce 2012, kdy jednou z možností pro páchání uvedených útoků bylo využít prostředek, distribuovaný přívrženci hnutí Anonymous, LOIC (Low Orbit Ion Cannon).



LOIC (Low Orbit Ion Cannon)[6]

Pomyslným nástupcem LOIC pak byl software HOIC (High Orbit Ion Canon), který byl vyvinut jako náhrada za LOIC.



HOIC (High Orbit Ion Canon)[7]

Jednání útočníků v tomto případě zcela jistě protiprávní je, neboť tito útočníci si byli vědomi nebo alespoň byli srozuměni s tím, že svým jednáním zasahují do práv jiných osob. V tomto případě by bylo možné využít prostředky trestního, správního i občanského práva.

Díky přijetí Úmluvy o kyberkriminalitě by mělo nejen v členských zemích EU docházet k harmonizaci zejména trestního práva a přijetí takových právních norem, které by měly být schopné postihnout DoS či DDoS útoky prostředky trestního práva té které země. K ochraně před těmito útoky a implementaci legislativních opatření vyzývá Kapitola II – Opatření, která mají být přijata na vnitrostátní úrovni, Oddíl 1 – Trestné činy proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů, Čl. 4 – Zasahování do dat, uvedené úmluvy:

1. *Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby podle jejích vnitrostátních právních předpisů bylo trestným činem, pokud je spácháno úmyslně neoprávněné poškození, vymazání, snížení kvality, pozměnění* ***nebo potlačení počítačových dat.***

2. *Strana si může vyhradit právo stanovit, že bude považovat jednání popsané v odstavci 1 za trestné, jen pokud způsobí závažnou škodu.*

Možnosti trestněprávního postihu v ČR

Ze znění ustanovení **§ 230 odst. 2** (Neoprávněný přístup k počítačovému systému a nosiči informací) TZK vyplývá:

Kdo získá přístup k počítačovému systému *nebo k nosiči informací a*

a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,
b) ***data*** *uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní,* ***potlačí****, sníží jejich kvalitu nebo je učiní neupotřebitelnými...*

Z uvedeného ustanovení vyplývá, že útočník páchající DoS či DDoS útok musí, aby byl případně trestně odpovědný, **neoprávněně získat přístup k počítačovému systému a následně v něm data potlačit.**[8]

V tomto případě de facto došlo ke spojení dvou samostatných článků (Kapitola II, Oddíl 1, **Čl. 2 – Nezákonný přístup** a **Čl. 4 – Zasahování do dat**) Úmluvy o kyberkriminalitě v ustanovení jedno.

Zákonodárce tímto de facto znemožnil postih pachatelů DoS či DDoS útoků prostředky trestního práva, neboť po pachateli je vyžadováno, aby **neoprávněně získal přístup k počítačovému systému**. Tato právní interpretace vyžadující získání neoprávněného přístupu k počítačovému systému tak umožňuje postih pachatele pouze pro jednání uvedené v Úmluvě o kyberkriminalitě v **Čl. 2 – Nezákonný přístup: „***Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby podle jejích vnitrostátních právních předpisů byl trestným činem, pokud je spáchán úmyslně,* ***neoprávněný přístup k celému počítačovému systému nebo jeho jakékoli části****.“*

Z technického hlediska při DoS či DDoS útocích **nedochází** k získání přístupu k počítačovému systému nebo jeho části, nebo to alespoň není primárním cílem.[9]

Z výše uvedených důvodů jsem přesvědčen o nutnosti včlenit do právní úpravy ČR samostatnou skutkovou podstatu trestného činu, která by chránila počítačový systém právě před útoky DoS, DDoS, DRDoS aj. a která by zejména respektovala ustanovení Úmluvy o kyberkriminalitě. Bylo by možné užít např. následující znění:

„Kdo bez oprávnění brání užívání počítačového systému....“

V současnosti by bylo teoreticky možné postihnout pachatele DoS a DDoS útoků za trestný čin dle **§ 228** (poškození věci) TZK.[10] Podmínkou pro využití institutu poškození věci by však musel být fakt, že by taková věc (tedy i počítačový systém) byla zničena, poškozena, nebo učiněna neupotřebitelnou. Uvedená podmínka však u tohoto typu útoku přichází v úvahu zpravidla pouze co se týče určité dočasné neupotřebitelnosti.

V této souvislosti však vyvstává i otázka, jak a jakým způsobem bude v případě poškození věci vyčíslována skutečně vzniklá škoda a na kom bude vymáhána.[11]

Mezi další skutkové podstaty, jichž by se útočník páchající útok typu DoS a DDoS mohl za určitých okolností dopustit, je možné zařadit § 272 (Obecné ohrožení), § 273 (obecné ohrožení z nedbalosti) TZK.

Z hlediska případného trestněprávního postihu pachatele DoS či DDoS útoků je významné i určení (identifikace) pachatele tohoto konkrétního trestného činu. Zůstává otázkou, **kdo všechno by měl být trestněprávně postižen jako pachatel**, který např. způsobil nedostupnost určité služby (např. webové aplikace).

---

[1] Blíže srov. např. MARCIÁ-FERNANDÉZ, Gabriel, Jesús E. DÍAZ-VERDEJO a Pedro GARCÍA-TEODORO. Evaluation of a Low-rate DoS Attack Against Application Servers. *Computers & Security*, 2008, roč. 27, č. 7-8, s. 335 – 354.

CARL, Glenn, Richard BROOKS a Rai SURESH. Wavelet Based Denial-of-Service Detection. *Computers & Security*, 2006, roč. 25, č. 8, s. 600 – 615

RAK, Roman a Radek KUMMER. Informační hrozby v letech 2007 – 2017. *Security magazín*, 2007, roč. 14, č. 1, s. 3.

[2] Dále například DoS útoky na webové stránky prezidentského úřadu, parlamentu, ministerstev, redakcí sdělovacích prostředků a dvou estonských bank - Estonsko (2007). *Estonia recovers from masive DDoS attack.* [online]. [cit. 4. 3.2010] Dostupné z: http://www.computerworld.com/s/article/9019725/Estonia_recovers_from_massive_DDoS_attack

[3] Blíže srov. JIROVSKÝ, Václav. *Kybernetická kriminalita. Nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, s. 66.

[4] Na tomto místě je třeba zmínit **Handshake -** proces, jehož úkolem je nastavit parametry komunikačního kanálu mezi dvěma subjekty před zahájením vlastní komunikace. Handshake je například používán v Internetu pro otevření TCP spojení (tzv. „**třícestný handshake**“, tj. výměna tří datagramů) a teprve poté následuje vlastní přenos dat. K navázání TCP spojení jsou požadovány tři oddělené kroky:

1. **Strana zahajující spojení (klient) vyšle TCP segment s nastaveným příznakem SYN.**
2. **Strana přijímající spojení (server) odpoví TCP segmentem s nastavenými příznaky SYN+ACK.**
3. **Klient odpoví TCP segmentem s nastaveným příznakem ACK**

Další TCP segmenty mají již nastaven pouze příznak ACK.

Blíže viz např. *TCP handshake krok za krokem.* [online]. [cit.18.8.2016]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=TCP-handshake-krok-za-krokem-3122000

Existují i další způsoby DoS útoku, např. „TearDrop“, „Nuke“, „Peer-to-Peer útok“, atd. Blíže srov. [online]. [cit.25.9.2010]. Dostupné z: http://cs.wikipedia.org/wiki/Denial_of_Service

[5] Může jít i o případ, kdy útočník rozešle hoax typu *„6. 6. 2016 od 12 do 13 budou letenky u Lufthansy zadarmo! Pro více informací klikni sem.“*

[6] *LOIC*. [online]. [cit.18.8.2016]. Dostupné z: https://i.ytimg.com/vi/QAbXGy0HbrY/maxresdefault.jpg

[7] *HOIC.* [online]. [cit.18.8.2016]. Dostupné z: https://npercoco.typepad.com/.a/6a0133f264aa62970b0167612ea130970b-pi

[8] Potlačením je rozuměna ta činnost, která je uvedena v čl. 4 Úmluvy o kyberkriminaltě.

[9] Pokud je např. k DoS či DDoS útoku využito PING Floodu, pak si je možné celou situaci představit jako neustálé volání (a následné zavěšení) na konkrétní telefonní číslo. Tím dojde k situaci, kdy napadené telefonní číslo nemá možnost uskutečnit hovor vlastní (dochází k blokaci funkce volání), avšak žádný z volajících (útočníků) nezíská žádné údaje uložené v napadeném telefonu.

[10]Viz § 228 odst. 1 TZK:

„Kdo zničí, poškodí nebo učiní neupotřebitelnou cizí věc, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.“

Škodou nikoli nepatrnou se rozumí škoda dosahující výše minimálně 5000 Kč (viz § 138 odst. 1 TZK)

[11]Bude tato škoda vymáhána na každém útočníkovi? Či bude tato škoda mezi útočníky „rozpočítána“?

4.14. Šíření závadového obsahu

V současné době lze vystihnout dva základní typy šíření závadového obsahu. Jedná se o **šíření zakázaných druhů pornografie** a o **šíření nenávistných a extremistických sdělení**.

V případě šíření **zakázaných druhů pornografie** jde zejména o šíření pornografického materiálu zobrazujícího styk se zvířetem a dále o šíření (resp. již pouhé držení) „dětské pornografie" (materiál zobrazující nebo jinak využívající dítě - osobu mladší 18 let, či osobu, jež se jeví být dítětem). Vlastních způsobů šíření existuje nepřeberné množství. Od prostého nabízení tohoto druhu pornografie ke stažení přes umisťování těchto materiálů do prostředí Internetu, šíření pomocí výměnných počítačových sítí, zasílání pomocí e-mailů apod.

Zneužívání dětí k výrobě pornografických materiálů a následná distribuce těchto materiálů je jednou z forem trestné činnosti, k jejímuž stíhání se zavázala většina států světa, bez ohledu na to, zda ratifikovala či neratifikovala Úmluvu o kyberkriminalitě. Byť je v této oblasti vyvíjena značná aktivita (nejen ze strany států, neziskových organizací a dalších osob), zůstává problém sexuálního zneužívání dětí online neustále aktuální.

Fenomén dětské pornografie provází společnost od prvních okamžiků, kdy bylo možné zachytit vlastní zneužívání na jakékoliv médium (papír, film aj.). Pravdou však je, že Internet umožnil masové šíření takovýchto materiálů mezi jednotlivými uživateli, stejně jako jejich větší míru anonymity.

Problém, který představuje Internet a kyberprostor, souvisí s dříve uvedeným tvrzením, že *„Internet nezapomíná".* Pokud je jakýkoli materiál nahrán, či přenesen prostřednictvím ICT, vždy může někde existovat kopie tohoto materiálu. Příkladem z České republiky, kdy sami uživatelé vytváří materiál, který zobrazuje nahé děti, může být filehostingový portál www.rajce.net. Tento portál rozhodně nebyl vytvořen jako prostředí pro distribuci jakéhokoliv pornografického či jinak závadného materiálu (k tomuto účelu existují jiné stránky), avšak uživatelé nerespektují ani základní pravidla služby rajce.net, zejména čl. 13, který uvádí:

*„**Obsah zobrazující nahé osoby, zejména mladší 18 let, je na Rajče povoleno umisťovat pouze do soukromých alb s heslem**; ostatní ustanovení těchto pravidel, zejména zákaz umísťovat na Rajče pornografický obsah nebo obsah neoprávněně zasahující do práva na ochranu osobnosti třetích osob, zůstávají i v takovém případě nedotčena."*

Přesto je možné na tomto webu nalézt celou řadu fotografií, byť vytvořených s dobrým úmyslem (například šíření fotografií mezi členy rodiny žijícími daleko od sebe), které jsou atraktivní pro kohokoliv, včetně případného útočníka. Díky dalším informacím, které jsou uveřejněny na tomto portálu, případně díky korelaci dat z jiných zdrojů dostupných online, je pro útočníka mnohem snazší například nalézt potenciální oběť.

Problém nepředstavuje ani tak nahrání fotografií nahých osob (s vědomím replikace dat), ale ta skutečnost, že tato data jsou otevřena všem uživatelům, nikoli pouze úzce omezené skupině (např. již zmiňované rodině).

Fotografie z rajce.net (fotografie je volně dostupná všem uživatelům)

Závěrem chci uvést, že rozhodně nemám nic proti focení dětí (případně sdílení některých fotografií s nejbližší rodinou) z důvodu uchování krásných vzpomínek. To, co mi vadí, je hloupé bezmyšlenkovité zpřístupňování těchto fotografií komukoliv v kyberprostoru.

Jedním z projektů z poslední doby, který se věnoval problematice zneužívání dětí online, byl počin nizozemské společnosti Terre des Hommes Netherlands (THN). Tato společnost vytvořila virtuální desetiletou Filipínku **Sweetie**. Sweetie deset dní komunikovala na internetových chatech a byla oslovena přibližně dvaceti tisíci muži. Tisíc z nich jí nabídlo peníze výměnou za online sex.

Šéf projektu Hans Guyt na tiskové konferenci v Haagu řekl, že tento typ zločinu vyžaduje nový způsob policejní práce. *"Predátoři ani jejich oběti nám při vyšetřování naproti nepřijdou,"* uvedl.

„Vytvořili jsme virtuální identitu, která představovala desetiletou Filipínku."

"Nikoho jsme nelákali, dokud nám sami nenabízeli peníze," řekl Guyt.

Aktivisté chtěli tímto způsobem upozornit na rostoucí problém zneužívání dětí prostřednictví webkamer. Tento fenomén nazývají "*internetovou sexuální turistikou.*"[1]

Možnosti trestněprávního postihu v ČR

V případě vytváření, držení či šíření materiálů, subsumovatelných pod pojem dětské pornografie, je možný postih uživatele dle **§ 192** (Výroba a jiné nakládání s dětskou pornografií), **§ 193** (Zneužití dítěte k výrobě pornografie) TZK. Trestná je i účast na pornografickém představení nebo jiném obdobném vystoupení, ve kterém účinkuje dítě (**§ 193a** TZK). Trestné je také získání přístupu k dětské pornografii prostřednictvím informační nebo komunikační technologie (**§ 192 odst. 2** TZK).

Trestný je i případ, kdy uživatel vyrobil, dovezl, vyvezl, provezl, nabídl, učinil veřejně přístupným, zprostředkoval, uvedl do oběhu, prodal nebo jinak jinému opatřil fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, v němž se projevuje násilí či neúcta k člověku, nebo které popisuje, zobrazuje nebo jinak znázorňuje pohlavní styk se zvířetem (**§ 191 odst. 1** TZK).

V případě **šíření nenávistných a extremistických sdělení** jde zejména o podporu a propagaci hnutí, které prokazatelně směřuje k potlačení práv a svobod člověka, projevy sympatií s takovým hnutím, hlásání rasové, etnické a národnostní, náboženské nebo třídní zášti či zášti vůči jiné skupině osob. Dále je sem řazeno šíření pomluv pomocí prostředků informačních technologií a v neposlední řadě též zasílání obtěžujících zpráv spadajících pod pojem stalking, resp. cyberstalking.

V těchto případech se může jednat o celou řadu trestných činů, jako jsou např. **§ 184** (Pomluva), **§ 353** (Nebezpečné vyhrožování), **§ 354** (Nebezpečné pronásledování), **§ 355** (Hanobení národa, rasy, etnické nebo jiné skupiny osob), **§ 356** (Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod), **§ 403** (Založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka), **§ 404** (Projev sympatií k hnutí směřujícímu k potlačení práv a svobod člověka), **§ 405** (Popírání, zpochybňování, schvalování a ospravedlňování genocidia) TZK.

---

[1] Blíže viz:

Computer-generated 'Sweetie' catches online predators. [online]. [cit.19.8.2016]. Dostupné z: http://www.bbc.com/news/uk-24818769

Nizozemci vytvořili virtuální dívku. Pomohla lapit přes tisíc pedofilů. [online]. [cit.19.8.2016]. Dostupné z: http://zpravy.idnes.cz/virtualni-holcicka-pomohla-lapit-tisic-pedofilu-fuu-/zahranicni.aspx?c=A131106_210025_zahranicni_zt

Video se **Sweetie** je dostupné online: https://www.youtube.com/user/sweetie.

4.15. Kybernetické útoky na sociálních sítích

V prostředí sociálních sítí je možné páchat většinu již dříve popsaných kybernetických útoků (např. malware, phishing, spam aj.). Důvodem, proč jsou kybernetické útoky na sociálních sítích popsány samostatně, je ta skutečnost, že se primárně (nikoliv však výhradně) odehrávají právě v prostředí sociálních sítí.

Mezi tyto specifické útoky je možné zařadit:

1. Kyberšikanu
2. Kybergrooming
3. Sexting
4. Kyberstalking

4.15.1. Kyberšikana

Šikana ve světě reálném spočívá ve snaze útočníka ublížit, ponížit, zesměšnit, urazit jiného, ať fyzicky či psychicky. Kyberšikana pak přenáší „klasickou šikanu" do světa virtuálního a umožňuje útočníkovi použít nástroje a prostředky, které mohou mít mnohem větší dopad na oběť než by tomu bylo ve světě reálném. Kyberšikana díky používání informačních a komunikačních technologií a trvanlivosti dat v kyberprostoru umožňuje opakované útoky na oběť, a to i v případě, že se oběť ve světě reálném geograficky značně vzdálila od místa, kde byla původně šikanována.

Kyberšikana může být propojena se šikanou „klasickou" (např. nahrávání fyzického napadení oběti a následné umístění tohoto útoku na web). Pro to, abychom mohli hovořit o kyberšikaně, je nutné, aby k šikanování byly použity informační a komunikační technologie či služby nabízené v kyberprostoru.

Mezi znaky kyberšikany je možné zařadit:

Pocit anonymity (Útočník má zpravidla pocit, že jej díky Internetu není možné dohledat.)

Neomezenost útoku (Díky ICT nemusí útočník řešit ani čas ani prostor pro svůj útok. Je možné šikanovat kdykoliv, odkudkoliv a kohokoliv. Vlastní útok také vyžaduje mnohem méně úsilí, než je tomu v případě šikany „klasické".)

Neomezený okruh útočníků (Na rozdíl od světa reálného, ve světě virtuálním nezáleží na věku, pohlaví, fyzické síle, postavení útočníka ve skupině aj. Šikanujícím může být jakákoli osoba.)

Neomezený prostor a prostředky (Internet poskytuje útočníkovi de facto neomezený prostor a prostředky pro šikanování. Útočník může opakovaně vyvěšovat urážlivé poznámky, komentáře fotografie a videa na různých portálech, sociálních sítích aj. Tyto materiály může vylepšovat a „zdokonalovat".)

Obtížná zjistitelnost (Na rozdíl od šikany klasické nemusí mít kyberšikana vnější projevy jako jsou podlitiny, chybějící peníze atd.)

Trvalost [Klasická šikana většinou sestává z jednotlivých útoků, které se sice opakují, ale dílčí útok pro oběť vždy skončí. U kyberšikany stačí např. jedna SMS, e-mail apod., oběť se k nim stále vrací (respektive jsou jí neustále připomínány, zasílány aj.), může tak i měsíce žít v traumatu. Útočné SMS, e-maily, fotografie apod. jsou trvalejší než jednotlivé fyzické útoky.][1]

Nejčastější projevy kyberšikany:

1. Pomlouvání, zastrašování, urážení, zesměšňování či jiné ztrapňování (sociální sítě, e-mail, SMS, chat, ICQ, Skype, hry aj.).
2. Pořizování zvukových záznamů, videí či fotografií, jejich grafické či jiné upravování a následné zveřejňování s cílem poškodit (zesměšnit) vybranou osobu.
3. Natáčení videí, při kterých je oběť napadána fyzicky či je jinak psychicky týrána a zesměšňována. Tato videa jsou následně zveřejněna online (jedná se o tzv. Happy Slapping).
4. Vytváření internetových stránek, sociálních účtů (úprava původních či vytváření nových profilů), diskusních portálů aj., které urážejí, pomlouvají nebo ponižují konkrétní osobu.
5. Zneužívání cizího účtu - krádež identity (e-mailového, diskuzního apod.).
6. Provokování a napadání uživatelů v diskuzních fórech (chatovací místnosti apod.).
7. Odhalování cizích tajemství.
8. Vydírání pomocí mobilního telefonu nebo Internetu.
9. Obtěžování a pronásledování voláním, psaním zpráv nebo prozváněním.[2]

Důsledky některých útoků:

Amanda Todd (15 let). Příběh, který se Amandě stal, je možné nalézt na jejím vlastním videu dostupném na youtube.com (qDIKB2_RpuY). Amanda spáchala sebevraždu.

Rebecca Ann Sedwicková (12 let), byla téměř rok šikanována na Internetu, spáchala v roce 2013 sebevraždu. Šikana začala poté, co Rebecca nějakou dobu chodila s jedním chlapcem. Její matka novinářům řekla, že dcera dostávala vzkazy jako: 'Jsi hnusná', 'Proč ještě žiješ?' a 'Jdi se zabít'. Situace se tak vyhrotila, že matka odhlásila dceru ze školy z Crystal Lake a zrušila její účet na Facebooku. Ze školy prý musela odejít. Zbytek roku ji matka učila doma. V září nastoupila do jiné školy. Zdálo se, že se vše obrací k lepšímu, a Rebecca v nové škole pookřála. Ale tajně se přihlásila k novým aplikacím včetně telefonního posílání zpráv Kik Messenger a Ask.fm a šikana začala nanovo poté, co se na Internetu začala dotazovat na nadváhu. Šerif Judd uvedl, že dívka byla na sociálních sítích "naprosto terorizována".[3]

Ghyslain Raza (14 let, Kanada), známý jako Star Wars Kid.

. Ghyslain Raza natočil sám sebe při předvádění bojové scény z Hvězdných válek. Snažil se napodobit postavu Dartha Maula. Spolužáci mu nahrávku ukradli a pro pobavení ostatních ji zveřejnili na Internetu. Během několika týdnů nahrávka oblétěla celý svět, byla mnohokrát upravována, vzniklo množství webů a blogů, na kterých byl chlapec zesměšňován. Ghyslainovi fanoušci napsali petici tvůrcům Hvězdných válek, aby byl obsazen do některé z epizod. Byl parodován dokonce v seriálech (např. South Park, American Dad, Veronica Mars). Ghyslain se psychicky zhroutil a musel se dlouhodobě léčit.[4]

Anna Halman (14 let, Polsko). Pět spolužáků podrobilo Annu před celou třídou sexuální šikaně (strhali z ní šaty a předstírali, že ji znásilňují). Celou scénu nahráli na mobil a vyhrožovali dívce, že nahrávku zveřejní na Internetu. To také později udělali, video umístili na stránku YouTube. Pro Annu to měla být pomsta za to, že s jedním z chlapců nechtěla chodit. Anna spáchala sebevraždu.[5]

Jessica Logan (18 let, USA). Po rozchodu zveřejnil Jessičin bývalý přítel její intimní fotografie, které mu poslala v době, kdy spolu ještě chodili. Jessica pak byla vystavena neustálému posměchu ze strany spolužáků. Útoky na ni ještě zesílily poté, co anonymně vystoupila v televizi, aby ostatní upozornila na rizika sextingu. Jessica spáchala sebevraždu.[6]

Možnosti trestněprávního postihu v ČR

Kyberšikana (stejně jako klasická šikana) sama o sobě není trestným činem ani přestupkem. Vždy záleží na jednání, kterým útočník šikanoval. Pokud toto jednání mělo podobu například fyzického ublížení oběti, jejímu vydírání či zastrašování, pak by mohlo přicházet v úvahu uplatnění například **§ 146** (Ublížení na zdraví) či **§ 145** (Těžké ublížení na zdraví), **§ 175** (Vydírání) TZK. V případě obtěžování a pronásledování osoby by bylo možné využít ustanovení **§ 354** TZK (Nebezpečné pronásledování). Avšak u kyberšikany, která se může projevovat například neustálým zesměšňováním, ztrapňováním a psychickým ubližováním prostřednictvím informačních a komunikačních technologií, bude aplikace některých výše uvedených ustanovení problematická, ne-li přímo nemožná.

4.15.2. Kybergrooming

Kybergrooming je jednání, které představuje psychickou manipulaci s osobou (typicky za použití sociálního inženýrství), realizovanou prostřednictvím Internetu či informačních a komunikačních technologií (např. mobilních telefonů aj.). Účelem kybergroomingu je vyvolat v oběti falešnou důvěru a přimět ji tak k osobní schůzce. Výsledkem této schůzky může být jakýkoli fyzický, sexuální či jiný útok na oběť. Oběťmi kybergroomingu mohou být děti, ale i dospělé osoby.[7] Nejčastějšími oběťmi jsou dle statistik dívky ve věku 13 – 17 let.[8]

„Psychická manipulace v rámci kybergroomingu probíhá obvykle delší dobu – od cca 3 měsíců po dobu několika let. Tato doba je přímo závislá na způsobu manipulace a na důvěřivosti oběti. Existují případy, kdy predátor manipuloval dítě po dobu 2–3 let, než došlo k osobnímu setkání a sexuálnímu zneužití. Je třeba rovněž zohlednit hranici zletilosti dítěte – útočník může s dítětem komunikovat v době, kdy bylo nezletilé, k útoku však dojde až po završení zletilosti (je zjevné, že trestní sazby za sexuální zneužití zletilého a nezletilého dítěte jsou velmi rozdílné).“[9]

Kybergrooming má různé etapy:

1. Vzbuzení důvěry a snaha izolovat oběť od okolí (útočník mění svoji identitu, je velmi trpělivý)
2. Podplácení dárky či různými službami, budování kamarádského vztahu
3. Vyvolání emoční závislosti oběti na osobě útočníka
4. Osobní setkání
5. Sexuální obtěžování, zneužití dítěte či jiný útok[10]

Rizikovou skupinu dětí tvoří:

1. *adolescenti/ teenageři* (zajímá je lidská sexualita, jsou ochotni o ní hovořit),
2. *děti s nízkou sebeúctou nebo nedostatkem sebedůvěry* (lze je snadněji citově či fyzicky izolovat),

3. *děti s emocionálními problémy, oběti v těžké životní situaci* (často hledají náhradu za své rodiče a potřebují pomocnou ruku),

4. *děti naivní a přehnaně důvěřivé* (jsou ochotnější zapojit se do online konverzace s neznámými lidmi, obtížněji rozpoznávají rizikovou komunikaci).

Možnosti trestněprávního postihu v ČR

Osoba dopouštějící se kybergroomingu může svým jednáním naplnit skutkovou podstatu některých trestných činů uvedených v trestním zákoníku. Zpravidla se bude, dle povahy jednání útočníka, jednat o trestné činy dle ustanovení **§ 168** (Obchodování s lidmi), **§ 171** (Omezování osobní svobody), **§ 175** (Vydírání), **§ 185** (Znásilnění), **§ 187** (Pohlavní zneužívání), **§ 201** (Ohrožování výchovy dítěte), **§ 209** (Podvod), **§ 353** (Nebezpečné vyhrožování), **§ 354** (Nebezpečné pronásledování) TZK.

Další z možných definic kybergroomingu uvádí, že jde o ***„takové chování uživatelů internetu, které má v dětské oběti vyvolat falešnou důvěru a přimět ji k osobní schůzce. Výsledkem této schůzky může být sexuální zneužití oběti,*** *fyzické násilí na oběti, zneužití oběti pro dětskou prostituci, k výrobě dětské pornografie apod.“*[11] V této souvislosti pak je možné využít speciálního ustanovení uvedeného v **§ 193b** (Navazování nedovolených kontaktů s dítětem) TZK.

4.15.3. Sexting

Jednou z podob nebezpečného chování zejména v prostředí sociálních sítí je tzv. sexting. Pojem sexting vznikl kombinací slov sex a texting, z čehož vyplývá i jeho význam. Jde o elektronické rozesílání textových zpráv, fotografií či videa se sexuálním obsahem. Takovýto materiál se sexuálním podtextem může být na sociální sítě či jiná datová úložiště nahráván přímo jeho samotnými autory nebo jiným uživatelem, který k takovému materiálu získal přístup. Nejčastěji se tak stane dobrovolným posíláním souborů se sexuálním obsahem, které jsou pořízeny samotným odesílatelem.

Následně (po ukončení komunikace, vztahu či z jiného důvodu) použije pachatel získaný choulostivý materiál k vyhrožování či vydírání. Pachatel v některých případech může pod pohrůžkou zveřejnění takovéhoto materiálu požadovat zaslání dalších fotografií či videa a psychickým nátlakem tak nutí poškozeného k výrobě a pořizování dalších materiálů, které pachatel vyžaduje buď pro vlastní potřebu, nebo se záměrem je sdílet na Internetu (v případě dětí je sdílí v komunitách zaměřených na dětskou pornografii). Druhou variantou pachatelova jednání je užití získaného materiálu k jinému nátlaku (např. obnovení partnerského vztahu, provozování sexuálních aktivit, zaslání finanční částky atp.) pod pohrůžkou zveřejnění již v minulosti získaných fotografií či videa (původně pachateli dobrovolně zaslaných poškozeným).

Z výsledků Výzkumu rizikového chování českých dětí v prostředí Internetu[12] 2014 zpracovaného Centrem prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci ve spolupráci s firmou Seznam.cz vyplývá, že 9,86 % dětí umístilo svou „sexy“ fotografii či video, na kterých jsou částečně nebo úplně nazí, na Internet. Z celkového počtu 28 232 respondentů 12,14 % uvedlo, že takovýto materiál někomu přes Internet/mobilní telefon poslalo.

U sextingu je podíl oběti na činu neoddiskutovatelný, neboť právě ona je osobou, která vytvořila předmětnou fotografii nebo video, avšak po odeslání tohoto materiálu ztrácí oběť naprostou kontrolu nad dalším „životem“ těchto dat.

Možnosti trestněprávního postihu v ČR

V případě zveřejnění fotek jiné osoby bez jejího souhlasu je možné, aby se dotčená osoba domáhala ochrany svých práv v rámci občanskoprávního řízení

V případě, že osoba uvádí o jiném nepravdivý údaj (tak jako tomu zřejmě bylo v případu *Roztahovaček*), který je způsobilý značnou měrou ohrozit jeho vážnost u spoluobčanů, zejména poškodit jej v zaměstnání, narušit jeho rodinné vztahy nebo způsobit mu jinou vážnou újmu, je možné využít **§ 184** (Pomluva) TZK.

Specifickým případem je pak situace, kdy jsou získávány a zneužívány audiovizuální materiály zobrazující dítě. Pokud útočník vyzývá dítě k vytvoření a následnému zaslání fotografií, videa či online streamování před web kamerou (které dítě zachycují nahé, obnažené či jinak vzbuzující sexuální vzrušení), může se dopustit trestného činu dle **§ 193** (Zneužití dítěte k výrobě pornografie) TZK.

Sexting se také velmi často projevuje tak, že pachatel nutí oběť posílat další materiály (fotky, videa, live stream aj.) s tím, že mu vyhrožuje, že pokud je nepošle, tak materiály, které již má v držení, zveřejní na Internetu nebo je zpřístupní jeho rodině či přátelům. Tím se dopustí trestného činu dle **§ 175 odst. 1** (Vydírání) TZK.

Osoba dopouštějící se sextingu může dále svým jednáním naplnit i skutkovou podstatu trestného činu dle **§ 192** (Výroba a jiné nakládání s dětskou pornografií) či **§ 201** (Ohrožování výchovy dítěte) TZK.

4.15.4. Kyberstalking

Kyberstalking je složenina slov kyber a stalking. Původně bylo slovo stalking používáno lovci divoké zvěře a znamenalo stopování zvěře až k jejímu uštvání. Stalking v té podobě, tak jak je chápán dnes, byl poprvé použit v 90. letech 20. století v rámci studie Meloye[13], který za stalking označil nebezpečné pronásledování známým či neznámým pachatelem, který pronásleduje oběť, a to takovým způsobem, že v ní vyvolává pocit nebezpečí, strachu. Toto pronásledování musí být dlouhodobější.

Kyberstalking je takové jednání, které spočívá v opakovaném kontaktování oběti například zasíláním SMS zpráv, e-mailů, telefonáty, VoIP, messengery aj. Jednání útočníka se zpravidla stupňuje a zpravidla vyvolá u oběti obavy o svoje soukromí, zdraví či život. Pro *kyberstalkery* je typická jejich vytrvalost a systematičnost, přičemž není neobvyklé, aby měl kyberstalker vytvořenou celou řadu falešných identit, které využívá ke kontaktování oběti. Kyberstalker může demonstrovat i svoji moc a sílu, například tím, že zveřejní informace ze života oběti, které může získat z různých online zdrojů.

Možnosti trestněprávního postihu v ČR

Stalking či kyberstalking je možné subsumovat, za splnění určitých podmínek, pod ustanovení **§ 354** (Nebezpečné pronásledování) TZK. Mezi základní podmínky patří, že útočník musí oběť dlouhodobě *„vytrvale prostřednictvím prostředků elektronických komunikací, písemně nebo jinak kontaktovat"* a toto jednání je způsobilé vzbudit v oběti důvodnou obavu o její život nebo zdraví nebo o život a zdraví osob jí blízkých. Okolností přitěžující dle **§ 354 odst. 2 písm. a)** TZK je ta skutečnost, že uvedený čin je spáchán na dítěti.

---

[1] Srov. *Co je to kyberšikana a jak se projevuje?* [online]. [cit.19.8.2016]. Dostupné z:

http://www.bezpecne-online.cz/pro-rodice-a-ucitele/teenageri-a-komunikace-na-internetu/co-je-to-kybersikana-a-jak-se-projevuje.html

Blíže o kyberšikaně viz např. *Kyberšikana I, II.* [online]. [cit.19.8.2016]. Dostupné z: https://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy

[2] Srov. dále: *Víte co je KYBERŠIKANA?* [online]. [cit.19.8.2016]. Dostupné z: http://www.policie.cz/clanek/vite-co-je-kybersikana.aspx

[3] *Dvanáctiletá dívka se zabila po téměř roční šikaně na internetu.* [online]. [cit.19.8.2016]. Dostupné z: https://www.novinky.cz/zahranicni/amerika/313386-dvanactileta-divka-se-zabila-po-temer-rocni-sikane-na-internetu.html

http://www.ceskatelevize.cz/ct24/svet/246314-dalsi-sebevrazda-kvuli-socialnim-sitim-divka-skocila-z-veze/

[4] *Kyberšikana I, II.* [online]. [cit.19.8.2016]. Dostupné z: https://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy

[5] *Kyberšikana I, II.* [online]. [cit.19.8.2016]. Dostupné z: https://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy

Dále pak: *Jessica Logan – The rest of the Story.* [cit.8.8.2016]. Dostupné z: http://nobullying.com/jessica-logan/

[6] Tamtéž.

[7] *Riziková komunikace: Kybergrooming* [online]. [cit.19.3.2014]. Dostupné z: http://www.e-nebezpeci.cz/index.php/rizikova-komunikace/kybergrooming

[8] CHOO, Kim-Kwang Raymond. *Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences* [online]. Canberra: Australian Institute of Criminology, c2009, [cit.19.3.2014]. ISBN 978-1-921532-33-7. Dostupné z: http://www.aic.gov.au/documents/3/C/1/%7b3C162CF7-94B1-4203-8C57-79F827168DD8%7drpp103.pdf

[9] KOPECKÝ, Kamil. *Nebezpečí zvané kybergrooming I*. In: Metodický portál inspirace a zkušenosti učitelů [online]. 2010. [cit.19.3.2014]. Dostupné z: http://clanky.rvp.cz/clanek/s/Z/9741/NEBEZPECI-ZVANE-KYBERGROOMING-I.html/#6a

[10] *Kybergrooming.* [online]. [cit.19.8.2016]. Dostupné z: http://www.policie.cz/clanek/vite-co-je-kybersikana.aspx

[11] KOPECKÝ, Kamil. *Nebezpečí zvané kybergrooming I*. In: Metodický portál inspirace a zkušenosti učitelů [online]. 2010. [cit. 2014-03-19]. Dostupné z: http://clanky.rvp.cz/clanek/s/Z/9741/NEBEZPECI-ZVANE-KYBERGROOMING-I.html/#6a

[12] *Výzkum rizikového chování českých dětí v prostředí internetu 2014.* [online]. [cit.19.8.2016]. Dostupné z: https://www.e-bezpeci.cz/index.php/ke-stazeni/doc_download/61-vyzkum-rizikoveho-chovani-eskych-dti-v-prostedi-internetu-2014-prezentace

[13] MELOY, Reid J. *STALKING (OBSESSIONAL FOLLOWING): A REVIEW OF SOME PRELIMINARY STUDIES.* [online]. [cit.3.10.2015]. Dostupné z: http://forensis.org/PDF/published/1996_StalkingObsessi.pdf

4.16. Identity theft

Identity theft je útok, při kterém dochází k odcizení virtuální identity[1], respektive jde o převzetí kontroly (trvalé, nebo dočasné) nad touto identitou. Motivem jednání útočníka může být finanční zisk, ale i jiné výhody, například přístup k informacím o jiných osobách, přístup k firemním datům ad., které jsou spojené s faktem, že útočník vystupuje jménem jiné osoby.

Jednání útočníka zpravidla spočívá v několika protiprávních jednáních najednou. Prvním protiprávním jednáním při identity theft je prolomení přístupových údajů či instalaci malware do počítačového systému oběti s cílem získat přístupu k virtuální identitě.

Po získání přístupu k identitě napadeného může dojít jak ke zneužití získaných informací pro útok na tuto osobu, tak ke zneužití identity s cílem útoku na jinou osobu. Vlastní útok na další oběť prostřednictvím odcizené identity je pro útočníka podstatně snazší, neboť tato druhá oběť standardně nemá žádné informace o záměně identity osoby (oběti první), s níž například pravidelně komunikuje a vyměňuje si citlivé údaje.

Pokud se v této souvislosti vrátím k problematice botnetů, tak jedním z typických úkolů malware, který je nainstalován při připojení počítačového systému do sítě botnet, je i automatická extrakce dat o uživatelích napadeného počítačového systému – tedy identity theft. Botmaster pak může kdykoliv získaná data využít tak, že se bude vydávat za určitou osobu či tato data prodá třetím osobám.[2]

Typicky jsou odcizené identity využívány k:

- provádění phishingových či malwarových útoků v rámci seznamu uživatelů, s nimiž osoba se odcizenou identitou komunikuje,
- rozesílání spamu,
- zisku informací, které nejsou veřejně dostupné (například informací o struktuře společnosti, nastavení bezpečnosti dalších služeb atd.),
- získávání přístupů do dalších služeb. Řada online služeb umožňuje, pouze na základě zadání e-mailové adresy, změnu hesla. Díky faktu, že útočník ovládá e-mailovou schránku napadeného, může dojít ke změně přístupových údajů i v celé řadě dalších služeb, které jsou s touto e-mailovou schránkou provázány.

Možnosti trestněprávního postihu v ČR

Pokud dojde k překonání bezpečnostního opatření a získání neoprávněného přístupu k identitě oběti, dojde k naplnění znaků trestného činu dle **§ 230 odst. 1** (Neoprávněný přístup k počítačovému systému a nosiči informací) TZK. Při použití malware ke stejnému účelu se útočník dopustí jednání dle § 230 odst. 2 TZK. Pokud je cílem identity theft získat sobě nebo jinému neoprávněný prospěch, je možné uplatnit i ustanovení **§ 230 odst. 3** TZK.
V případě, že útočník odcizí identitu s cílem oklamat jiného, tedy vyvolat v něm omyl s cílem obohatit se, mohlo by takové jednání být posouzeno i dle **§ 209** (Podvod) TZK.

---

[1] Virtuální identitou se rozumí jakákoliv totožnost či avatar využívaný osobou pro interakci v rámci kyberprostoru (Např. e-mail, účet na sociální síti, ve hře, v různých online tržištích, v rámci počítačového systému aj.). Nezáleží na skutečnosti, zda je virtuální indentita pravá či falešná, tedy jestli představuje reálnou či osobu, či jde o zcela uměle vytvořenou identitu, bez reálného základu.

[2] Blíže viz PLOHMANN, Daniel, Elmar GERHARDS-PADILLA a Felix LEDER. *Botnets: Detection, Measurement, Disinfection & Defence.* ENISA, 2011, s. 22 [online]. [cit.17.5.2015]. Dostupné z: https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence

4.17. APT (Advanced Persistent Threat)

Pojem APT je doslovně možné přeložit jako „pokročilá a trvalá hrozba“. Jedná se o dlouhodobý systematický kybernetický útok, zaměřený na cílový počítačový systém, respektive na ICT cílové organizace. K vlastnímu útoku jsou využívány různé techniky a poměrně rozsáhlé zdroje, přičemž typicky může docházet k napadání sekundárních cílů (počítačových systémů organizace např. opakovanými DoS či jinými útoky) s cílem odvedení pozornosti od primárního cíle (infiltrace společnosti malwarem), který je následně napaden.

„APT je obvykle zaměřena na vytěžení strategicky hodnotných utajených či neveřejných dat, omezení akceschopnosti cíle, nebo zaujetí pozice, která umožňuje budoucí realizaci zmiňovaného. Uskutečnění akcí, které definici APT naplňují, je spojeno s vysokou úrovní odborných znalostí, značnými finančními zdroji a schopností dlouhodobě se adaptovat na jednání oběti útoku. Charakteru APT tak nabývají především státní aktéři, potažmo jimi řízená a sponzorovaná uskupení, nebo specializované skupiny organizovaného zločinu.“[1]

Vlastní APT útok se typicky skládá:

- ze zisku informací o cíli útoku (sběr informací z otevřených zdrojů; využití sociálního inženýrství aj.)
- z vlastního útoku:
  - Výběr vhodných prostředků (malware, tvorba krycích identit aj.)
  - V případě, že je systém napadnutelný zvenčí, dochází k jeho napadání
  - Pokud je systém zvenčí nedostupný, dochází k využívání jiných technik zkombinovaných se sociálním inženýrstvím (např. Spear phishing, Identity Theft aj.)
- z převzetí kontroly nad některými počítačovými systémy, upevnění pozice uvnitř napadené počítačové sítě
- ze sběru dat a informací a jejich zasílání útočníkovi
- z vytěžení dat

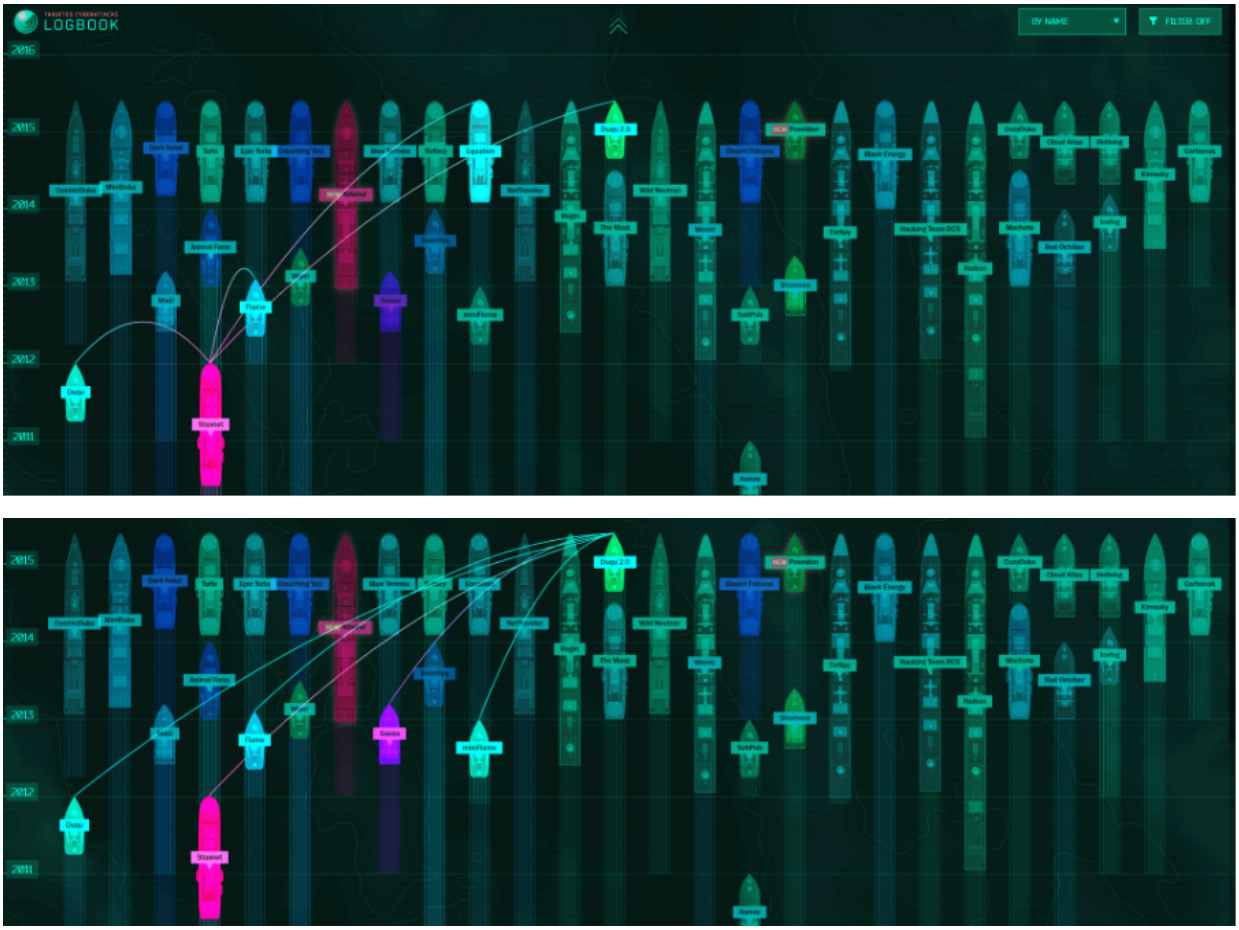
Útočníci v průběhu APT útoku mohou využívat další různé typy útoků na zvolený cíl, v závislosti na datech a informacích, jež získali.

APT je možné zobrazit pomocí jeho životního cyklu:

Průběh APT útoku[2]

Vlastní APT útok může trvat od několika měsíců po řadu let a součástí útoku mohou být i poměrně dlouhá období, kdy je aktivita útočníků minimální. Výjimkou není ani vedení velkého počtu obdobných operací proti různým cílům současně.[3]

Na stránce společnosti Kasperky Lab (https://apt.securelist.com/#firstPage) jsou graficky znázorněny známé APT útoky, včetně uvedení informací o tom, kdy se poprvé objevil vzorek útočného malware, kdy byl objeven útok APT, kde primárně působí (geolokační informace, primárně napadané operační systémy, počet cílů aj.) atp. Následující dva printscreeny zobrazují primární vazbu malware Stuxnet (mimo jiné i na Duqu 2.0.) a následně vazbu Duqu 2.0 na další malware.



Zobrazení ATP útoků včetně jejich provázanosti[4]

Možnosti trestněprávního postihu v ČR

Případný trestněprávní postih útočníka či útočníků provádějících APT útok pak zcela závisí na jejich jednání, které může mít např. podobu distribuce malware, některého z phishingových útoků, Identity Theft aj.

---

[1] *Advanced Persistant Threat.* [online]. [cit.20.8.2016]. Dostupné z: https://www.isouvislosti.cz/advanced-persistent-threat

[2] *Advanced Persistant Threat – life cycle.* [online]. [cit. 20. 8. 2016]. Dostupné z: https://upload.wikimedia.org/wikipedia/commons/7/73/Advanced_persistent_threat_lifecycle.jpg

[3] Blíže viz: *Advanced Persistant Threat.* [online]. [cit. 20. 8. 2016]. Dostupné z: https://www.isouvislosti.cz/advanced-persistent-threat

Advanced Persistant Threat (APT). [online]. [cit. 20. 8. 2016]. Dostupné z: http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT

Advanced Persistent Threats: How They Work. [online]. [cit.10.7.2016]. Dostupné z: https://www.symantec.com/theme.jsp?themeid=apt-infographic-1

How do APTs work? The Lifecycle of Advanced Persistent Threats (Infographic). [online]. [cit. 10. 7. 2016]. Dostupné z: https://blogs.sophos.com/2014/04/11/how-do-apts-work-the-lifecycle-of-advanced-persistent-threats-infographic/

[4] *Targeted cyberattacks logbook.* [online]. [cit.10.7. 2016]. Dostupné z: https://apt.securelist.com/#secondPage

4.18. Kyberterorismus

V souvislosti s kybernetickými útoky nelze opomenout ani terorismus, který představuje jednu z aktuálních globálních hrozeb a lze sledovat jeho dynamický nárůst a rozšiřování do celého světa.

Terorismus můžeme rozdělit podle formy na *letální* a *neletální* formy, kde první skupina se vyznačuje použitím běžných prostředků pro realizaci násilí (*konvenční* – útoky páchané pomocí běžně dostupných bojových prostředků, např. střelných zbraní a *nekonvenční* – zneužití zbraní hromadného ničení). V oblasti Internetu jsou však **běžnější neletální formy terorismu**[1] nebo útoky, při kterých jsou využívány moderní nástroje v kombinaci s letálními prostředky.

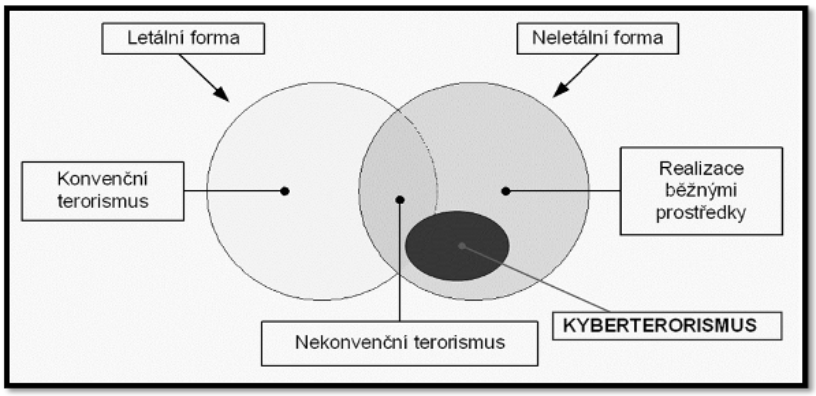
Konvenční forma neletálního terorismu zahrnuje níže uvedené podskupiny:

- *Neozbrojený terorismus*.

- *Kyberterorismus*, který patří mezi největší nebezpečí 21. století. Principem je především zneužívání ICT (včetně Internetu) jako prostředku a prostředí pro uskutečnění útoku. Jedná se, podobně jako u klasického konvenčního teroristického útoku, o plánovanou činnost motivovanou zpravidla politicky či nábožensky a realizovanou spíše malými, ne vojensky organizovanými strukturami. Cílem těchto skupin je především ovlivnění veřejného mínění. Vzhledem k rychlému šíření informačních a komunikačních technologií po celém světě představuje kyberterorismus významné nebezpečí a je teroristickými skupinami využíván ve stále rostoucí míře.[2]

- *Mediální terorismus*, při němž dochází k plánovanému zneužívání hromadných sdělovacích prostředků a jiných psychologických prostředků za účelem ovlivnění názorů celé populace, nebo cílových skupin obyvatelstva.

Nejvýstižněji tento vztah charakterizuje schéma uvedené na následujícím obrázku.



Zobrazení forem terorismu včetně kyberterorismu

Globální charakter informatického a telekomunikačního prostředí umožňuje předávání informací a koordinaci teroristických aktivit v rámci celého světa. Uvádí se, že např. útok na WTC v New Yorku byl organizován právě s využitím Internetu.

Je možno uvést i další případy zneužití Internetu pro šíření závadných informací nebo pro psychologické operace související s mediálním terorismem. Internet se podstatnou měrou podílí na šíření propagandy, ideologie či zastrašování například v podobě zveřejnění poprav zajatců online[3], získávání a mobilizaci nových aktivistů, sympatizantů či sponzorů, obhajobě teroristických činů a podněcování jednotlivců k jejich páchání. Internetové servery teroristických skupin často obsahují návody na výrobu improvizovaných zbraní, nebo propagandu zacílenou na mladší generaci.

Internet poskytuje zcela výjimečné možnosti extremistickým a teroristickým skupinám i jednotlivcům, a to zejména v oblasti rychlé a relativně utajené komunikace, kdy slouží ke vzájemné výměně informací a pokynů k plánování a koordinaci akcí nebo převodu finančních prostředků.

Bezmála všechny teroristické skupiny a organizace provozují své internetové stránky. Obvykle jsou zveřejňovány v několika jazykových mutacích a nechybí ani speciální stránky zaměřené na děti a ženy obsahující pohádky či komiksy, do nichž jsou zapracovány například příběhy sebevražedných atentátníků.[4]

Webové stránky TravelWest.info po napadení útočníky

Možnosti trestněprávního postihu v ČR

Z hlediska trestního práva pak uvedené jednání může naplňovat skutkové podstaty trestných činů **§ 311 odst. 2** (Teroristický útok), **§ 355** (Hanobení národa, rasy, etnické nebo jiné skupiny osob), **§ 356** (Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod), **§ 364** (Podněcování k trestnému činu), **§ 403** (Založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka) a **§ 404** (Projev sympatií k hnutí směřujícímu k potlačení práv a svobod člověka) TZK.

---

[1] Nicméně je možné si představit i kombinaci těchto útoků. Blíže viz např.:

Exclusive: Computer Virus Hits U.S. Drone Fleet. [online]. [cit.10.7.2016]. Dostupné z: https://www.wired.com/2011/10/virus-hits-drone-fleet/

[2] JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007, s. 129

[3] **Předložené URL není cenzurováno a obsahuje drastické záběry!** Viz např.:

WATCH: ISIS Downs Prisoners Alive & Blows Hostages Up With RPG & Kills Others With Explosives - Graphic video. [online]. [cit.20.8.2016]. Dostupné z: https://www.zerocensorship.com/uncensored/isis/drowns-prisoners-alive-blows-hostages-up-with-rpg-kills-others-with-explosives-graphic-video-132382

Disturbing ISIS video shows militants beheading four prisoners and gunman executing shoppers at market. [online]. [cit.20.8.2016]. Dostupné z: http://www.mirror.co.uk/news/world-news/disturbing-isis-video-shows-militants-7306017

[4] JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007, s. 138

Dále viz např.:

Cyber Terrorism: How Dangerous is the ISIS Cyber Caliphate Threat? [online]. [cit.20.8.2016]. Dostupné z: http://www.govtech.com/blogs/lohrmann-on-cybersecurity/Cyber-Terrorism-How-Dangerous-is-the-ISIS-Cyber-Caliphate-Threat.html

Islamic State Hacking Division. [online]. [cit.20.8.2016]. Dostupné z: https://ent.siteintelgroup.com/index.php?option=com_customproperties&view=search&task=tag&bind_to_category=content:37&tagId=698&Itemid=1355

5. SHRNUTÍ/ HLAVNÍ VÝSTUPY Z KAPITOLY

ℹ️

SHRNUTÍ/ HLAVNÍ VÝSTUPY Z KAPITOLY

- Značná část kyberkriminality využívá či přenáší notoricky známé druhy protiprávního jednání (např. podvody, porušování práv autorských, krádeže, šikanu aj.) do prostředí digitálního, ve kterém je lze páchat „lépe, rychleji, efektivněji“ než ve světě reálném. Mezi ryze kybernetické útoky je možné zařadit např. hacking, DoS a DDoS útoky, botnety aj.
- S rozvojem služeb postavených na principu as-a-service vznikla i v prostředí kyberkriminality řada platforem (typicky undergroundových, darknet fór), kde jsou nabízeny služby, které je možné označit za **Crime-as-a-service** (cybercrime-as-a-service). Dochází tedy ke vzniku *„malware* či *underground economy“,* která poskytuje téměř jakémukoli uživateli prostředky ke spáchání kybernetických trestných činů.
- V kapitole jsou představeny základní kybernetické útoky. Prezentován je typický modus operandi, jakož mi možnosti trestně právního postihu za tato jednání.
- Kybernetickou kriminalitu lze definovat jako jednání namířené proti počítači, případně počítačové síti, nebo jako jednání, při němž je počítač použit jako nástroj pro spáchání trestného činu. Neopomenutelnou skutečností pro to, aby bylo možné uplatnit definici kyberkriminality, je fakt, že počítačová síť, respektive kyberprostor je pak prostředím, v němž se tato činnost odehrává.

🗝️

KLÍČOVÁ SLOVA K ZAPAMATOVÁNÍ

- sociální inženýrství
- botnet
- malware
- ransomware
- spam
- scam
- phishing
- pharming
- podvod
- hacking
- cracking
- DoS, DDoS
- APT

❓

KONTROLNÍ OTÁZKY

- Jak se projevuje sociální inženýrství?
- Co to je botnet a jak funguje?
- Jaké jsou tytické topologie botnetů?
- Je možné trestněprávně postihnout vlastníka botnetu?
- Co to je malware?
- Jaké jsou nejčastější projevy malware?
- Jaké jsou nejčastější infekční vektory malware?
- Co to je ransomware a jak se typicky projevuje?
- Co to je phishing a jakým způsobem je tento útok nejčastěji veden?
- Jaký je rozdíl mezi phishingem a pharmingem?
- Co to je hacking?
- Jak se projevuje cracking?
- Jaký je rozdíl mezi hackingem a crackingem?
- Co to je DoS útok a jak probíhá?
- Jaký je rozdíl mezi DoS a DDoS?
- Co vše je možné zařadit pod šíření závadového obsahu?
- Co to je APT?

6. Závěr

Jsem pevně přesvědčen o tom, že kyberprostor se nesmí stát prostředím, kde by bylo možné beztrestně páchat jakoukoliv trestnou činnost. Na druhou stranu je třeba nastavit pravidla a podmínky tak, aby se nestal ani prostředím, v němž bude převládat cenzura a represe. Vyvážení těchto dvou rovin je klíčovým předpokladem pro uplatňování a zejména respektování pravidel v kyberprostoru, ať již legálních, či morálních.

Pokud jde o aplikaci případných trestněprávních norem na určité druhy kybernetických útoků, je třeba uvést, že není možné stíhat prostředky trestního práva sebenebezpečnější jednání, které není zakotveno v rámci trestních kodexů té které země. Trestní právo je prostředkem *ultima ratio* a jako takové musí být značně precizní, aby nezasahovalo do práv a svobod osob ve větší míře, než je nezbytně nutné.

Vedle státu se ochranou kyberprostoru a jeho uživatelů zabývají různé soukromé organizace. Domnívám se, že pokud chceme účinně s kyberkriminalitou bojovat, mělo by dojít k efektivnější spolupráci soukromých organizací (zejména IT odborníků, CSIRT týmů aj.) se složkami veřejné (státní) správy, či s orgány činnými v trestním řízení tak, aby bylo možné včas a adekvátně reagovat na stále sofistikovanější formy kyberkriminality či kyber útoků.

Jak jsem uvedl v úvodu: *„Život bez informačních a komunikačních technologií je pro naši společnost již nemyslitelný, respektive nemožný.“*

Mým názorem je, že nemá smysl se oprošťovat od ICT a služeb, které jsou s těmito technologiemi spojené. Účelem této monografie nebylo donutit uživatele odinstalovat si Facebook a nepoužívat Google či jiné služby. Smyslem bylo upozornit na možná rizika spojená s užíváním informačních a komunikačních technologií a služeb s nimi spojených. V této souvislosti je třeba připomenout citát *Scientia est potentia* (**vědění je moc, v poznání a znalostech je síla, vědění je síla**). V případě ICT a služeb s nimi spojených je třeba poznat, co tyto technologie a služby představují, co činí a k čemu slouží.

Redukce negativních jevů v kyberprostoru a snaha o změnu tak nutně musí začít u koncových uživatelů, neboť v kyberprostoru jsou to právě oni, kdo je typickou první obětí útočníka. Zároveň jsou uživatelé autoritou, která může definovat, jaké služby, data či informace budou v kyberprostoru vyhledávány, ukládány a poskytovány.

Věřím, že výchova a vzdělávání uživatelů má být nezbytnou součástí prostupu informačních a komunikačních technologií do našich životů. Budování informační gramotnosti by mělo být neodmyslitelně spojeno s tvorbou, distribucí a podporou produktů, či služeb, které jsou s informačními a komunikačními technologiemi spojeny. Vlastní vzdělávání v této oblasti, či spíše seznamování se s možnými hrozbami, riziky a negativy IT, by mělo být součástí výuky všech forem studia na všech úrovních školství.

“Nikdo nedělá větší chybu než ten, kdo

nedělá nic v domnění, že to málo, co udělat může, nemá smysl.“

Edmund Burke

7. Použitá literatura

1. *10 Most Notorious Hacking Groups.* [online]. [cit.15.7.2016]. Dostupné z: https://www.hackread.com/10-most-notorious-hacking-groups/

2. *7 Types of Hacker Motivations.* [online]. [cit.16.8.2015]. Dostupné z: https://blogs.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations/

3. *7 Types of Hackers You Should Know.* [online]. [cit.16.8.2015]. Dostupné z: https://www.cybrary.it/0p3n/types-of-hackers/

4. *Advanced Persistant Threat – life cycle.* [online]. [cit. 20. 8. 2016]. Dostupné z: https://upload.wikimedia.org/wikipedia/commons/7/73/Advanced_persistent_threat_lifecycle.jpg

5. *Advanced Persistant Threat (APT).* [online]. [cit. 20. 8. 2016]. Dostupné z: http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT

6. *Advanced Persistant Threat.* [online]. [cit.20.8.2016]. Dostupné z: https://www.isouvislosti.cz/advanced-persistent-threat

7. *Advanced Persistent Threats: How They Work.* [online]. [cit.10.7.2016]. Dostupné z: https://www.symantec.com/theme.jsp?themeid=apt-infographic-1

8. *Adware.* [online]. [cit.10.8.2016]. Dostupné z: http://www.mhsaoit.com/computer-networking-previous-assignments/324-lesson-16-h-the-secret-history-of-hacking

9. *Android Ransomware now targerts your Smart TV, Too!* [online]. [cit.14.8.2016]. Dostupné z: https://thehackernews.com/2016/06/smart-tv-ransomware.html

10. *Android version market share distribution among smartphone owners as of May 2016.* [online]. [cit.14.8.2016]. Dostupné z: http://www.statista.com/statistics/271774/share-of-android-platforms-on-mobile-devices-with-android-os/

11. BALIGA, Arati, Liviu IFTODE a Xiaoxin CHEN. Automated Containment of Rootkits Attacks. *Computers & Security*, 2008, roč. 27, č. 7-8, s. 323 – 334.

12. BAUDIŠ, Pavel. Programy typu rootkit. Další hrozba pro Windows. *CHIP*, 2005, č. 7, s. 14

13. *Beware of Fake Android Prisma Apps Running Phishing, Malware Scam* [online]. [cit.14.8.2016]. Dostupné z: https://www.hackread.com/fake-android-prisma-app-phishing-malware/

14. *Botnet – Historical List of Botnets.* [online]. [cit.15.8.2016]. Dostupné z: http://www.liquisearch.com/botnet/historical_list_of_botnets

15. *Botnet.* [cit.8.7.2016]. Dostupné z: http://research.omicsgroup.org/index.php/Botnet

16. *Botnet.* [online]. [cit.15.7.2016]. Dostupné z: https://en.wikipedia.org/wiki/Botnet

17. *Botnets.* [online]. [cit.15.7.2016]. Dostupné z: https://www.youtube.com/watch?v=-8FUstzPixU&index=2&list=PLz4vMsOKdWVHb06dLjXS9B9Z-yFbzUWI6

18. *Botnety: nová internetová hrozba.* [online]. [cit.15.7.2016]. Dostupné z: http://www.lupa.cz/clanky/botnety-internetova-hrozba/

19. *Bots and Botnets – A growing Threat.* [online]. [cit.11.8.2016]. Dostupné z: https://us.norton.com/botnet/

20. *Buffalo Spammer jde na 7 let za mříže kvůli rozesílání nevyžádané pošty.* [online]. [cit.14.8.2016]. Dostupné z: http://technet.idnes.cz/buffalo-spammer-jde-na-7-let-za-mrize-kvuli-rozesilani-nevyzadane-posty-13i-/tec_reportaze.aspx?c=A040528_28629_tec_aktuality

21. CARL, Glenn, Richard BROOKS a Rai SURESH. Wavelet Based Denial-of-Service Detection. *Computers & Security*, 2006, roč. 25, č. 8, s. 600 – 615

22. CHOO, Kim-Kwang Raymond. *Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences* [online]. Canberra: Australian Institute of Criminology, c2009, [cit.19.3.2014]. ISBN 978-1-921532-33-7. Dostupné z: http://www.aic.gov.au/documents/3/C/1/%7b3C162CF7-94B1-4203-8C57-79F827168DD8%7drpp103.pdf

23. *Co je to botnet a jak se šíří?* [online]. [cit.15.7.2016]. Dostupné z:

24. *Co je to kyberšikana a jak se projevuje?* [online]. [cit.19.8.2016]. Dostupné z: http://www.bezpecne-online.cz/pro-rodice-a-ucitele/teenageri-a-komunikace-na-internetu/co-je-to-kybersikana-a-jak-se-projevuje.html

25. *Čo sa skrýva v prílohe podvodných e-mailov?* [online]. [cit.15.8.2016]. Dostupné z: https://blog.nic.cz/2014/07/23/co-sa-skryva-v-prilohe-podvodnych-e-mailov-2/

26. *Co znamená přípona souboru SCR.* [online]. [cit.14.8.2016]. Dostupné z: http://www.solvusoft.com/cs/file-extensions/file-extension-scr/

27. *Combating Cybercrime in a Digital Age.* [online]. [cit.7.5.2016]. Dostupné z: https://www.europol.europa.eu/ec3

28. *Computer-generated 'Sweetie' catches online predators.* [online]. [cit.19.8.2016]. Dostupné z: http://www.bbc.com/news/uk-24818769

29. *Convicted spammer challenging Va. law* [online]. [cit.14.8.2016]. Dostupné z: http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va_N.htm

30. *Cyber Terrorism: How Dangerous is the ISIS Cyber Caliphate Threat?* [online]. [cit.20.8.2016]. Dostupné z: http://www.govtech.com/blogs/lohrmann-on-cybersecurity/Cyber-Terrorism-How-Dangerous-is-the-ISIS-Cyber-Caliphate-Threat.html

31. *Cybercrime*. [online]. [cit.1.2.2015]. Dostupné z: http://www.britannica.com/EBchecked/topic/130595/cybercrime/235699/Types-of-cybercrime; aj.

32. *Digital Doom's Digi World*, 2008. ISSN 1802-047X. [online]. [cit.14.8.2016]. Dostupné z: http://www.ddworld.cz/software/windows/jak-se-krade-pomoci-internetu-phishing-v-praxi.html

33. *Distribuované výpočty.* [online]. [cit.2.11.2013]. Dostupné z: http://dc.czechnationalteam.cz/

34. *Disturbing ISIS video shows militants beheading four prisoners and gunman executing shoppers at market.* [online]. [cit.20.8.2016]. Dostupné z: http://www.mirror.co.uk/news/world-news/disturbing-isis-video-shows-militants-7306017

35. DOČEKAL, Daniel. Bruce Schneier: *Internet věcí přinese útoky, které si neumíme představit.* [online]. [cit.10.8.2016]. Dostupné z: http://www.lupa.cz/clanky/bruce-schneier-internet-veci-prinese-utoky-ktere-si-neumime-predstavit/

36. DOČEKAL, Daniel. *Google: Adware napadá miliony zařízení a poškozuje inzerenty, weby i uživatele.* [online]. [cit.10.8.2016]. Dostupné z: http://www.lupa.cz/clanky/google-adware-napada-miliony-zarizeni-a-poskozuje-inzerenty-weby-i-uzivatele/

37. Dodatkový protokol. ETS No. 189 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189

38. DODGE, Ronald. C., Curtis CARVE a Aaron J. FERGUSON. Phishing for User Security Awareness. *Computers & Security*, 2007, roč. 26, č. 1, s. 73 – 80.

39. *Dvanáctiletá dívka se zabila po téměř roční šikaně na internetu.* [online]. [cit.19.8.2016]. Dostupné z: https://www.novinky.cz/zahranicni/amerika/313386-dvanactileta-divka-se-zabila-po-temer-rocni-sikane-na-internetu.html

40. *Estonia recovers from masive DDoS attack.* [online]. [cit. 4. 3.2010] Dostupné z: http://www.computerworld.com/s/article/9019725/Estonia_recovers_from_massive_DDoS_attack

41. *Exclusive: Computer Virus Hits U.S. Drone Fleet.* [online]. [cit.10.7.2016]. Dostupné z: https://www.wired.com/2011/10/virus-hits-drone-fleet/

42. *Fight against cyber crime: cyber patrols and Internet investigation teams to reinforce the EU strategy.* [online]. [cit.10.7.2016]. Dostupné z: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1827

43. *Flappy Bird Clones Help Mobile Malware Rates Soar.* [online]. [cit.14.8.2016]. Dostupné z: http://www.mcafee.com/us/security-awareness/articles/flappy-bird-clones.aspx

44. *FLocker Mobile Ransomware Crosses to Smart TV.* [online]. [cit.14.8.2016]. Dostupné z: http://blog.trendmicro.com/trendlabs-security-intelligence/flocker-ransomware-crosses-smart-tv/

45. *France drops controversial 'Hadopi law' after spending millions.* [online]. [cit.15.7.2016]. Dostupné z: https://www.theguardian.com/technology/2013/jul/09/france-hadopi-law-anti-piracy aj.

46. *Fridge caught sending spam emails in botnet attack.* [online]. [cit.17.5.2016]. Dostupné z: http://www.cnet.com/news/fridge-caught-sending-spam-emails-in-botnet-attack/

47. GONZÁLES-TALAVÁN, Guillermo. A Simple, Configurable SMTP Anti-spam Filter: Greylists. *Computers & Security*, 2006, roč. 25, č. 3, s. 229 – 236.

48. GOODMAN, Marc. *A vision of crimes in the future.* [online]. [cit.13.11.2014]. Dostupné z: https://www.ted.com/talks/marc_goodman_a_vision_of_crimes_in_the_future#t-456071

49. *Google says the best phishing scams have a 45-percent success rate.* [online]. [cit. 14.8.2016]. Dostupné z: https://www.engadget.com/2014/11/08/google-says-the-best-phishing-scams-have-a-45-percent-success-r/

50. GREENBERG, Andy. *Hackers remotely koll a Jeep on the highwaty – with me in it.* [online]. [cit.4.5.2016]. Dostupné z: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

51. GRIFFITHS, Mark. Computer Crime and Hacking: a Serious Issue for the Police? *The Police Journal,* 2000, roč. 73, č. 1, s. 18 –24.

52. GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Praha: Auditorium, 2008

53. *Hackeři se vydávají za Anonymous a hrozí útokem českým firmám.* [online]. [cit.16.8.2015]. Dostupné z: http://www.lupa.cz/clanky/hackeri-vydavajici-se-za-anonymous-hrozi-utokem-na-ceske-firmy-chteji-zaplatit/

54. *Hackeři zaútočili na uživatele Facebooku*. [online]. [cit.16.8.2015]. Dostupné z: http://tech.ihned.cz/c1-37133210-hackeri-zautocili-na-uzivatele-facebooku-chteli-jejich-hesla

55. HILL, Kashmir. *These two Diablo III players stole virtual armor and gold — and got prosecuted IRL*. [online]. [cit.10.8.2015]. Dostupné z: http://fusion.net/story/137157/two-diablo-iii-players-now-have-criminal-records-for-stealing-virtual-items-from-other-players/

56. *Historical list of botnets.* [online]. [cit.15.8.2016]. Dostupné z: http://jpdias.me/botnet-lab//history/historical-list-of-botnets.html

57. *Historical Maps of Computer Networks*. [online]. [cit.10.7.2016]. Dostupné z: https://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/historical.html

58. HOŘEJŠÍ, Jaromír. *Falešný exekuční příkaz ohrožuje uživatele českých bank.* [online]. [cit.15.8.2016]. Dostupné z: https://blog.avast.com/cs/2014/07/17/falesny-exekucni-prikaz-ohrozuje-uzivatele-ceskych-bank-2/

59. *How do APTs work? The Lifecycle of Advanced Persistent Threats (Infographic).* [online]. [cit. 10. 7. 2016]. Dostupné z: https://blogs.sophos.com/2014/04/11/how-do-apts-work-the-lifecycle-of-advanced-persistent-threats-infographic/

60. *How to use Wireshark to capture, Filter and inspect Packets.* [online]. [cit.15.7.2016]. Dostupné z: http://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/

61. *Islamic State Hacking Division.* [online]. [cit.20.8.2016]. Dostupné z: https://ent.siteintelgroup.com/index.php?option=com_customproperties&view=search&task=tag&bind_to_category=content:37&tagId=698&Itemid=1355

62. *Jessica Logan – The rest of the Story.* [cit.8.8.2016]. Dostupné z: http://nobullying.com/jessica-logan/

63. JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 2. aktualiz. vyd. Praha: AFCEA, 2015, s. 57 a 73. [online]. [cit.10.7.2016]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/

64. JIROVSKÝ, Václav a Oldřich KRULÍK. Základní definice vztahující se k tématu. *Security magazín*, 2007, roč. 14, č. 2, s. 47.

65. *Judge, 69, who downloaded child porn facing 'catastrophic humiliation'.* [online]. [cit.1.9.2009]. Dostupné z: http://news.sciencemag.org/social-sciences/2015/02/facebook-will-soon-be-able-id-you-any-photo

66. Kevin Mitnick Case: 1999. [online]. [cit.2.11.2011]. Dostupné z: http://www.encyclopedia.com/doc/1G2-3498200381.html

67. KOLOUCH, Jan, Pavel BAŠTA a kol. *CyberSecurity*. Praha: CZ.NIC, 2019. ISBN 978-80-88168-31-7.

68. KOLOUCH, Jan. Evolution of Phishing and Business Email Compromise Campaigns in the Czech Republic. In: *Academic and Applied Research in Military and Public Management Science*. Budapest: National University of Public Service, 2018, s.83-100. ISSN 2498-5392

69. KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016. ISBN 978-80-88168-15-7

70. KOLOUCH, Jan a Andrera KROPÁČOVÁ. Ransomware. In: ZHUANG, Xiaodong. *Recent Advances in Computer Science: Proceedings of the 19th International Conference on Computers*. B.m.: B.n., 2015, s. 304-307. Recent Advances in Computer Engineering Series, [Nr. 32]. ISBN 978-1-61804-320-7. ISSN 1790-5109.

71. *Kybergrooming.* [online]. [cit.19.8.2016]. Dostupné z: http://www.policie.cz/clanek/vite-co-je-kybersikana.aspx

72. *Kyberšikana I, II.* [online]. [cit.19.8.2016]. Dostupné z: https://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy

73. *Kyberšikana I, II.* [online]. [cit.19.8.2016]. Dostupné z: https://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy

74. LEVY, Steven. *Hackers: Heroes of the Computer Revolution* Sebastopol, CA: O'Reilly edia, s. 32-41. ISBN 978-1449388393.

75. LI, Tao, GUAN, Zhihong, WU, Xianyong. Modeling and Analyzing the Spread of Active Worms Based on P2P Systems. *Computers & Security*, 2007, roč. 26, č. 3, s. 213 – 218.

76. *Malware, mayhem, and the McColo takedown.* [online]. [cit.14.8.2016]. Dostupné z: http://betanews.com/2008/11/13/malware-mayhem-and-the-mccolo-takedown/

77. MARCIÁ-FERNANDÉZ, Gabriel, Jesús E. DÍAZ-VERDEJO a Pedro GARCÍA-TEODORO. Evaluation of a Low-rate DoS Attack Against Application Servers. *Computers & Security*, 2008, roč. 27, č. 7-8, s. 335 – 354.

78. MATĚJKA, Michal. *Počítačová kriminalita.* Praha: Computer Press, 2002

79. MELOY, Reid J. *STALKING (OBSESSIONAL FOLLOWING): A REVIEW OF SOME PRELIMINARY STUDIES.* [online]. [cit.3.10.2015]. Dostupné z: http://forensis.org/PDF/published/1996_StalkingObsessi.pdf

80. MINAŘÍK, Pavel. *Wireshark – Paketová analýza pro všechny.* [online]. [cit.18.8.2016]. Dostupné z: https://www.systemonline.cz/it-security/wireshark-paketova-analyza-pro-vsechny.htm

81. MITNICK, Kevin D. a William L., SIMON. *Ghost in the wires: my adventures as the world's most wanted hacker*. New York: Little, Brown & Co, 2012. ISBN 9780316037723.

82. MITNICK, Kevin D. *The art of intrusion: the real stories behind the exploits of hackers, intruders & deceivers*. Indianapolis: Wiley, c2006. ISBN 0-471-78266-1.

83. MUELLER, Robert. [online]. [cit.3.4.2013]. Dostupné z: https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies

84. *Největší hackerský útok potvrzen. V ohrožení jsou stovky miliónů uživatelů.* [online]. [cit.16.8.2015]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/405260-nejvetsi-hackersky-utok-potvrzen-v-ohrozeni-jsou-stovky-milionu-uzivatelu.html

85. *New Ransomware Encrypts Your Game Files.* [online]. [cit.14.8.2016]. Dostupné z: https://techcrunch.com/2015/03/24/new-ransomware-encrypts-your-game-files/

86. NIGAM, Ruchna. *A timeline of Mobile Botnets.* [online]. [cit.12.7.2016]. Dostupné z: https://www.botconf.eu/wp-content/uploads/2014/12/2014-2.2-A-Timeline-of-Mobile-Botnets-PAPER.pdf

87. *OWASP, XSS* [online]. [cit.15.7.2016]. Dostupné z: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

88. *Password Sniffer Spy.* [online]. [cit.18.8.2016]. Dostupné z: http://securityxploded.com/password-sniffer-spy.php

89. *Phishing Activity Tresnds Report.* [online]. [cit.14.8.2016]. Dostupné z: https://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf

90. *Phishing by the Numbers: Must-Know Phishing Statistics 2016.* [online]. [cit. 14.8.2016]. Dostupné z: https://blog.barkly.com/phishing-statistics-2016

91. PLETZER, Valentin. Demaskovaný spyware. *CHIP*, 2007, č. 10, s. 116 – 120.

92. PLOHMANN, Daniel, Elmar GERHARDS-PADILLA a Felix LEDER. *Botnets: Detection, Measurement, Disinfection & Defence.* ENISA, 2011. [online]. [cit.17.5.2015], s. 14. Dostupné z: https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence

93. *Policejní ransomware.* [online]. [cit.14.8.2016]. Dostupné z: https://www.f-secure.com/documents/996508/1018028/multiple_ransomware_warnings.gif/8d4c9ca2-fc77-433d-ac16-7661ace37f88?t=1409279719000

94. *Postřehy z bezpečnosti: Ransomware šestkrát jinak.* [online]. [cit.14.8.2016]. Dostupné z: https://www.root.cz/clanky/postrehy-z-bezpecnosti-ransomware-sestkrat-jinak/

95. *POŽÁR, Josef. Informační bezpečnost*. Plzeň: Aleš Čeněk, 2005

96. *Pozor na zprávu o údajné neuhrazené pohledávce - jedná se o podvod.* [online]. [cit.15.8.2016]. Dostupné z: https://www.csirt.cz/page/2073/pozor-na-zpravu-o-udajne-neuhrazene-pohledavce---jedna-se-o-podvod/

97. *Pozor na zprávu o výzvě k úhradě před exekucí - jedná se o podvod.* [online]. [cit.15.8.2016]. Dostupné z: https://www.csirt.cz/news/security/?page=87

98. PROSISE, Chris a Kevin MANDIVA. *Incident response & komputer forensic, second edition.* Emeryville: McGraw-Hill, 2003

99. RAK, Roman a Radek KUMMER. Informační hrozby v letech 2007 – 2017. *Security magazín*, 2007, roč. 14, č. 1, s. 4.

100. *Ransomware.* [online]. [cit.14.8.2016]. Dostupné z: https://www.trendmicro.com/vinfo/us/security/definition/ransomware

101. *Riziková komunikace: Kybergrooming* [online]. [cit.19.3.2014]. Dostupné z: http://www.e-nebezpeci.cz/index.php/rizikova-komunikace/kybergrooming

102. SCHNEIER, Bruce. *Crime: The Internet's Next Big Thing.* [online]. [cit.6.11.2007]. Dostupné z https://www.schneier.com/crypto-gram/archives/2002/1215.html

103. SCHNEIER, Bruce. *The Internet of Things Will Turn Large-Scale Hacks into a Real World Disasters.* [online]. [cit.10.8.2016]. Dostupné z: https://motherboard.vice.com/read/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster

104. SCHNEIER, Bruce. *The Seven Types of Hackers.* [online]. [cit.16.8.2015]. Dostupné z: https://www.schneier.com/blog/archives/2011/02/the_seven_types.html

105. SCHRYEN, Guido. The Impact that Placing Email Addresses on the Internet Has on the Receipt of Spam: An Empirical Analysis. *Computers & Security*, 2007, roč. 26, č. 5, s. 361 – 372.

106. Selfmite - *Android SMS worm Selfmite returns, more aggressive than ever.* [online]. [cit.14.8.2016]. Dostupné z: http://www.pcworld.com/article/2824672/android-sms-worm-selfmite-returns-more-aggressive-than-ever.html

107. *Škodlivý kód cílí na mobily, šíří se jako lavina.* [online]. [cit.17.5.2016]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/401956-skodlivy-kod-cili-na-mobily-siri-se-jako-lavina.html

108. *Sledování zásilky České pošty aneb nová havěť.* [online]. [cit.14.8.2016]. Dostupné z: http://www.viry.cz/sledovani-zasilky-ceske-posty-aneb-nova-havet/

109. SMEJKAL, Vladimír, Tomáš SOKOL a Martin VLČEK. *Počítačové právo.* Praha: C. H. Beck, 1995

110. Smejkal, Vladimír. Kriminalita v prostředí informačních systémů a rekodifikace trestního zákoníku. Trestněprávní revue, 2003, roč. 2, č. 6, s. 161.

111. SMEJKAL, Vladimír. *Kybernetická kriminalita.* Plzeň: Aleš Čeněk, 2015

112. *Spam Statistics and Facts.* [online]. [cit.14.8.2016]. Dostupné z: http://www.spamlaws.com/spam-stats.html

113. *Spam statistics*. [online]. [cit.14.8.2016]. Dostupné z: https://www.spamcop.net/spamstats.shtml

114. STRAUS, Jiří a kol. *Kriminalistická metodika.* Plzeň: Aleš Čeněk, 2006

115. *Stuxnet.* [online]. [cit.23.7.2016]. Dostupné z:https://cs.wikipedia.org/wiki/Stuxnet

116. *Targeted cyberattacks logbook.* [online]. [cit.10.7. 2016]. Dostupné z: https://apt.securelist.com/#secondPage

117. TAYLOR, Harriet. *How the „Internet of Things" could be fatal.* [online]. [cit.17.6.2016]. Dostupné z: http://www.cnbc.com/2016/03/04/how-the-internet-of-things-could-be-fatal.html

118. *TCP handshake krok za krokem.* [online]. [cit.18.8.2016]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=TCP-handshake-krok-za-krokem-3122000

119. *The Internet Organised Crime Threat Assessment (iOCTA) 2014.* [online]. [cit.10.8.2015]. Dostupné z: https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta

120. *The Malware Museum @ Internet Archive*. [online]. [cit.17.5.2016]. Dostupné z: https://labsblog.f-secure.com/2016/02/05/the-malware-museum-internet-archive/

121. *The testimony of an ex-hacker.* [online]. [cit.26.9.2008]. Dostupné z: http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/testimony.html

122. *The very first mobile malware: how Kaspersky Lab discovered Cabir*. [online]. [cit.29.6.2015]. Dostupné z: http://www.kaspersky.com/about/news/virus/2014/The-very-first-mobile-malware-how-Kaspersky-Lab-discovered-Cabir

123. Tinba: *W32. Tinba (Tinybanker)*. [online]. [cit.15.8.2016]. Dostupné z: https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_w32-tinba-tinybanker.pdf

124. *Tip of the month July 2016 – Avoid getting hooked by Phishing*. [online]. [cit.14.8.2016]. Dostupné z: http://www.intermanager.org/cybersail/tip-of-the-month-july-2016-avoid-getting-hooked-by-phishing/

125. *Top Spammer Sentenced to Nearly Four Years.* [online]. [cit.14.8.2016]. Dostupné z: http://www.pcworld.com/article/148780/spam.html

126. Úmluva o kyberkriminalitě. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

127. *United Nations Manual on the prevention and control of computer-related crime.* [online]. [cit.20.8.2016]. Dostupné z: http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf

128. *Války síťových robotů– jak fungují sítě botnets.* [online]. [cit.15.7.2016]. Dostupné z: http://tmp.testnet-8.net/docs/h9_botnet.pdf

129. *Víte co je KYBERŠIKANA?* [online]. [cit.19.8.2016]. Dostupné z: http://www.policie.cz/clanek/vite-co-je-kybersikana.aspx

130. *Výzkum rizikového chování českých dětí v prostředí internetu 2014.* [online]. [cit.19.8.2016]. Dostupné z: https://www.e-bezpeci.cz/index.php/ke-stazeni/doc_download/61-vyzkum-rizikoveho-chovani-eskych-dti-v-prostedi-internetu-2014-prezentace

131. *Warning! Over 900 Milion Android Phones Vulnerable to New „QuadRooter" Attack.* [online]. [cit.10.8.2016]. Dostupné z: https://thehackernews.com/2016/08/hack-android-phone.html

132. *WATCH: ISIS Downs Prisoners Alive & Blows Hostages Up With RPG & Kills Others With Explosives - Graphic video.* [online]. [cit.20.8.2016]. Dostupné z: https://www.zerocensorship.com/uncensored/isis/drowns-prisoners-alive-blows-hostages-up-with-rpg-kills-others-with-explosives-graphic-video-132382

133. **WILSON Tracy, V.** *How Phishing Works.* [online]. [cit.14.8.2016]. Dostupné z: http://computer.howstuffworks.com/phishing.htm

134. Xshqi - *Android Worm on Chinese Valentine's day.* [online]. [cit.14.8.2016]. Dostupné z: https://securelist.com/blog/virus-watch/65459/android-worm-on-chinese-valentines-day/

135. *Yahoo řeší, jestli má hacker opravdu údaje o 200 milionech účtů.* [online]. [cit.16.8.2015]. Dostupné z: http://www.lupa.cz/clanky/yahoo-resi-jestli-hacker-opravdu-ma-udaje-o-200-milionech-tamnich-uctu/

136. YAR, Majid. Computer Hacking: Just Another Case of Juvenile Delinquency? *The Howard Journal*, 2005, roč. 44, č. 4, s. 387 – 399.

137. ZETTER, Kim. *Is It Possible for Passengers to Hack Commwrcial Aircraft?* [online]. [cit.5.5.2016]. Dostupné z: https://www.wired.com/2015/05/possible-passengers-hack-commercial-aircraft/

138. *Znovu se objevily podvodné zprávy*. [online]. [cit.15.8.2016]. Dostupné z: https://www.csirt.cz/news/security/?page=97