UNIVERZITA JANA AMOSE KOMENSKÉHO PRAHA

BAKALÁŘSKÉ KOMBINOVANÉ STUDIUM

2012 – 2013

BAKALÁŘSKÁ PRÁCE

Pavla Najšlová

Kyberterorismus, co o něm víme?

Praha 2013

Vedoucí bakalářské práce práce: Ing. Michaela Havlová

JAN AMOS KOMENSKY UNIVERSITY PRAGUE

BACHELOR COMBINED
STUDIES

2012 - 2013

BACHELOR THESIS

Pavla Najšlová

Cyberterrorism, and what we know about it?

Prague 2013

The Bachelor Thesis Work Supervisor: Ing. Michaela Havlová

Prohlášení

Prohlašuji, že předložená bakalářská práce je mým původním autorským dílem, které jsem vypracovala samostatně. Veškerou literaturu a další zdroje, z nichž jsem při zpracování čerpala, v práci řádně cituji a jsou uvedeny v seznamu použitých zdrojů.

Souhlasím s prezenčním zpřístupněním své práce v univerzitní knihovně.

V Praze dne …….. *Jméno autorky* .....

Poděkování

Chtěla bych poděkovat své vedoucí práce Ing. Michaele Havlové za pomoc při zpracovávání bakalářské práce, trpělivost a ochotu.

Anotace

Bakalářská práce je zaměřena na kyberterorismus a informace o něm. V teoretické části se zabývá obecně kyberprostorem, kyberterorismem, stručnou historií, hrozbami a útočníky kyberterorismu. Praktická část pojednává o analýze informovanosti obyvatel o kyberterorismu a návrhu na její zlepšení.

Klíčové pojmy

Kyberterorismus, kyberteroristi, kyberteroristické útoky, hrozby, dotazníková šetření

Annotation

This bachelors work is focused on cyberterrorism and information about it. In the theory part we discuss the cyberspace, cyberterrorism, history, threats and the cyberterrorists.
In the practical part, on the other hand, we discuss the analysis about awareness of citizens about the cyberterrorism and ideas about improving the awareness of citizens.

Key words

Cyberterrorism, cyberterrorist, cyberterrorist attacks, surveys, threats

OBSAH

ÚVOD

Výběr mé bakalářské práce byl prostý. Kyberterorismus, kybernetické útoky, kybernetická kriminalita a kybernetická šikana jsou populární témata dnešní doby, ale opravdu jsou tolik známá, jak by měla být?

Terorismus je známé téma většině obyvatel planety Země, ale kyberterorismus již stejný zájem nemá, ač by měl. I proto jsem výběr tématu směřovala právě k němu.

Možnost kontaktu s počítačem, internetem a kyberprostorem mi byla dána od raného mládí a proto k tomuto tématu mám velmi blízko.

Asi každý pátý z nás se někdy snažil najít heslo od osobních složek u některé z osob ve svém okolí. Důvody mohly být různé. Zášť, zvědavost, snaha uškodit nebo naopak nezištně pomoci. Kde, ale končí hranice nevinného „hraní si“, kde začíná hranice kriminality a kde se kriminalita mění v terorismus?

Ve své bakalářské práci bych chtěla shrnout definici kyberterorismu, historii jeho vzniku a souvislost s terorismem jako takovým, jaké hrozby přináší kyberterorismus lidem, přiblížení kyberteroristy a jeho příklad. Práce bude zakončena analýzou informovanosti obyvatel o kyberterorismu a návrhem na jejím zvýšení.

TEORETICKÁ ČÁST

1. KYBERPROSTOR

První síťové propojení počítačů proběhlo v roce 1968. To, co nejvíce posunulo lidskou populaci k využití virtuálního světa, byl knihtisk. Respektive, byl to právě knihtisk, který se zapříčinil o tento krok.

Díky tištěným knihám se jedinci oddělovali od společnosti. Vzali si knihu a mohli být, jak se říká, ve svém světě. Jenomže pouze v jednosměrném. Informace plynuly směrem ke čtenáři, nikoli od čtenáře do knihy.

Průlomem byla výpočetní technika a internet. Na internetu můžete být kýmkoliv. V konečné fázi, i mnou. Stejně jako roste anonymita jedince v davu, roste i anonymita ve virtuálním světě. Člověk, který je v reálném, světě ustrašený a nevýrazný bývá ve virtuálním světě drsným a tvrdým rváčem. Mnohdy lidé hledají odpovědi na své životní otázky právě zde a časem pro ně reálný svět vymizí. Protože „tam“ existuje jejich lepší já.

A tak vznikl tak zvaný kyberprostor. Prostor bez zábran, výčitek, nutností. Prostor, kde se scházejí všechna potřebná témata reálného života. V dnešní době můžete sedět v obýváku a zařídit vše pouze pomocí internetu. Banky, telefony, práci a i nákupy. Vše jednoduše, díky kyberprostoru.

Lidem vyhovuje život bez zábran, nikdo jim neříká, že něco nesmějí, nebo smějí. Nikdo jim neříká, jak se mají chovat.

Obrázek 1 MATRIX

ZDROJ: Stiv101. In: *Matrix tekst efekat na tutorial* [online]. 2012 [cit. 2013-01-25]. Dostupné z: http://stiv101.deviantart.com/art/Matrix-tekst-efekat-na-tutorial-308966687

K lepšímu pochopení kyberprostoru se dá užít film, jistě všem známý. A to MATRIX. Film z roku 1999, který atakoval snad všechna kina na světě. Absolutní fikce o světě, kde můžete všechno. O světě, se kterým Vás propojí jeden jediný kabel. Na druhou stranu, o světě, jenž má být reálný a perfektní fikce zdánlivě spokojeného života, kterou jste dříve prožívali, se změní v peklo.

Zamyslíme-li se nad tímto filmem, není daleko od pravdy. Samozřejmě, je, jak se říká, ad absurdum, ale přesto, v kyberprostoru můžeme všechno, na rozdíl od filmu, toto „všechno“ neovládáme myšlenkami.

Jenomže se vznikem kyberprostoru vznikla i nová nebezpečí. Čím více anonymity, tím více odvahy.

2. KYBERTERORISMUS

2.1 Kyberterorismus jako součást terorismu

Než začneme zařazovat kyberterorismum, měli bychom si vysvětlit pojmy k tomu potřebné. Terorismus jako takový vyznačuje, dle Bezpečnostní strategie České republiky z roku 2011, metodu násilného prosazování politických cílů.[1]

Dle Ministerstva Vnitra je oficiální pojem terorismus známý od roku 1980, kdy v USA byla definována nejčastěji používaná definice a to taková, že „*Terorismus je propočítané použití násilí nebo hrozby násilím, obvykle zaměřené proti nezúčastněným osobám, s cílem vyvolat strach, jehož prostřednictvím jsou dosahovány politické, náboženské nebo ideologické cíle. Terorismus zahrnuje i kriminální zločiny, jež jsou ve své podstatě symbolické a jsou cestou k dosažení jiných cílů, než na které je kriminální čin zaměřen*.“[2]

Terorismus můžeme dělit na několik typů např. dle motivů, pohnutek, způsobu vykonání. Nejčastěji zmiňované typy terorismu jsou níže uvedené čtyři typy. S kyberterorismem jich je již pět. Asi jako první a nejdůležitější typ terorismu by bylo vhodné zmínit tak zvaný politický terorismus, jde o typ terorismus, kde je motivem nespokojenost s politickým systémem. Druhým typem je tak zvaný kriminální terorismus, který je založen na organizovaném zločinu. Třetím typem terorismu je náboženský terorismus, zde již z názvu vyplývá motiv, a to náboženství. Za čtvrtý typ terorismu se dá považovat psychotický typ terorismu. Zde spíše, než o dosažení cíle jde o druhotný cíl a to paniku a nahnání strachu. Teroristé bývají psychicky nemocní. A výčet by mohl pokračovat. Pro nás je ovšem hlavní, že se mezi typy se řadí i kyberterorismus.

[1] KOLEKTIV AUTORŮ POD VEDENÍM MZVČR. *Bezpečnostní strategie 2011*. Praha, 2011. ISBN 978-80-7441-005-5

[2] MVČR. ODBOR BEZPEČNOSTNÍ POLITIKY. *Definice pojmu terorismus* [online]. 2009 [cit. 2013-01-12]. Dostupné z: http://www.mvcr.cz/clanek/definice-pojmu-terorismus.aspx

2.2 Definice, vysvětlení pojmu

„Kyberterorismus je konvergencí terorismu a kyberprostoru obecně chápaný jako nezákonný útok nebo nebezpečí útoku proti počítačům, počítačovým sítím a informacím v nich skladovaným v případě, že útok je konán za účelem zastrašit nebo donutit vládu, nebo obyvatele k podporování sociálních nebo politických cílů.“ americká analytička D. E. Denning. Tato citace mluví za vše. Čtyřřádková definice popisující kyberterorismus jako takový. Ovšem, víceméně popisující pouze část.

Kyberterorismus je tedy, podle této analytičky chápán jako útok prostřednictvím kyberprostoru napadající kritickou infrastrukturu.

Kritickou infrastrukturou je myšlena výrobní i nevýrobní sféra, která, kdyby přestala fungovat, ohrozilo by to závažně bezpečnost státu, životů a zdraví obyvatel a zajištění jejich základních životních potřeb.

Jenomže vždy nemusí jít pouze o kritickou infrastrukturu. Relativně by se o kyberterorismu dalo hovořit i u útoku, kdy se díky programu vypuštěnému do kyberprostoru, aktivistům podařilo nahromadit neuvěřitelné množství dat různých uživatelů. Více než 6 milionů přístupových hesel k účtům osob na sociální síti. Případ známý jako Linkedln[3].

Jiná definice mluví tak, že kyberterorismus využívá informační technologie k útoku na civilisty a upozorňuje na jejich příčiny. To může znamenat, že používají informační technologie, jako jsou například počítačové systémy nebo telekomunikací, jako nástroj pro organizování tradičních útoků. Častěji kyberterorismus odkazuje k útoku na informační technologie samotné, a to způsobem, který by radikálně narušil síťové služby. Například může kyberterorismus zakázat síťové nouzové systémy nebo se nabourat do sítí domácí kritické finanční infrastruktury.

[3] STANISLAV KUŽEL. *Kybernetická kriminalita: Od hackerů ke kybernetickým válkám* [online]. Bispiral, s.r.o., 2012 [cit. 2013-01-15]. BusinessIT ebooks. Dostupné z: http://www.businessit.cz/ebooks/kyberkriminalita.pdf

Obrázek 2 Kyberterorismus ve státech třetích zemí

ZDROJ: Terorismus v Indii. In: *Indii ohrožuje kyberterorismus* [online]. 2008 [cit. 2013-01-15]. Dostupné z: http://terorismusvindii.blogspot.cz/2008/10/indii-ohrouje-kyber-teror_13.html

Kyberterorismus je obrovskou bezpečnostní hrozbou současnosti. O tom nemůže být sporu.

2.3 Historie vzniku

Kyberterorismus se objevuje již od osmdesátých let dvacátého století. Ovšem jde spíše o kybernetické útoky, kybernetickou šikanu, spam nebo kybernetickou kriminalitu.

Extrémní nárůst kybernetických útoků se objevil po teroristickém útoku na USA 11. Září 2001. Mezi aktivity té doby patřilo spamování e-mailových schránek, hacking vládních portálů, nemocnic, finanční sféry apod. Samozřejmě za účelem vyvolání paniky nebo ohrožení životů lidí.

Jako příklad se dá užít útok z roku 1996. Počítačový hacker rozeslal zprávy s rasistickým podtextem do celého světa rádoby pod záštitou poskytovatele internetových služeb z Massachusetts, záštita samozřejmě žádná nebyla. Počítačový hacker byl po celou dobu, před zraky lidí, pro zákaz rasistických hnutí.

V roce 1999 bylo zasaženo NATO útoky hackerů.

V roce 2000 se neznámý pachatel dostal do Maroochy Shire v Austrálii a prostřednictvím řídicího systému vypustil miliony galonů odpadní vody na město.[4]

Móda kyberterorismu, dá-li se tomu tak říkat, roste s módou kyberprostoru.

[4] SHANDRA. *Cyber Terrorism* [online]. [cit. 2013-01-05]. Dostupné z: http://cyberterrorismlaw.blogspot.cz/2012/03/history.html

2.4 Technika versus lidská síla

Nebudeme se zabývat dobou, kdy lidé neznali žádné nástroje, tuto dobu úplně vynecháme. Dalo by se totiž polemizovat nad otázkami, zda v pravěku opravdu měli jen kyje a pazourky, nebo měli technologie, které se objevovaly na malbách v jeskyních.

Obrázek 3 P. Dvorský Pračlověk otesávající pazourek

ZDROJ: DVORSKÝ, P. Projektové vyučování. In: *Virtuální univerzity v informační společnosti*[online]. 2010 [cit. 2013-01-15]. Dostupné z: http://www.projevypk.cz/index.php?text=1&iddoc=77&id1=8

Ano, studie říkají, že v pravěku měli opravdu pouze kyje, pazourky a na podobných principech pracující nástroje, které nebylo nijak těžké vyrobit či zpracovat, ale malby se neobjevily samy od sebe. Tuto dobu tedy přeskočíme a podíváme se na dobu našich prababiček.

Dříve vše, co bylo potřeba, vykonávali lidé. Pracovali na polích jen s pomocí rýčů, lopat a motyk. Oblečení šili ručně. Máslo stloukali taktéž jen pomocí rukou a pár nástrojů, které vyrobili, opět ručně. Co potřebovali, to si vyrobili, nebo postup pozměnili, aby byla možnost vytvoření daného výsledku. Když se potřebovali spojit s ostatními, využili možnosti zavolat z okna, nebo na větší vzdálenosti poslali syna, „jdi a vyřiď." Když už dálka neumožňovala poslat potomka, nebo zavolat z okna, poslal se dopis. Ten poslíček donesl či dovezl adresátovi

Postupem času a vývoje lidstva se vyvíjela i technika a technologie. Lidé se pomalu začali vyměňovat za stroje. Na polích sice dál dělali zemědělci, jen už jim pomáhaly první traktory, které sice nebyli extra spolehlivé, ale kus práce za ně udělali. A lidem se ulevilo. Švadleny už neměly tolik rozpíchané prsty, protože jim začal

pomáhat šicí stroj. Pořád u něj ovšem musely sedět. Sice zde bylo pár strojů, které rapidně ulehčily práci, ale na druhou stranu, pořád je někdo musel obsluhovat. Lidská síla byla pořád potřeba.

V dnešní době, době technologií a technických vymožeností, všude, kde je to možné, vidíme techniku, techniku zastupující davy lidí. Pomocí technologií ji zastupuje pouze jedna osoba, která vesměs pouze zmáčkne pár tlačítek. S tím je spojená i rychle rostoucí nezaměstnanost a problémy s ní spojené. Lidé si začali nejen díky nezaměstnanosti všímat jejich, částečné, neupotřebovatelnosti. Vznik manufaktur tomu nasvědčuje. Jako dárek více ocení mýdlo z manufaktury, než mýdlo vyráběné po tisících kusech, pouze zmáčknutím tlačítka.

Propojíme-li si výše uvedený text a význam celé bakalářské práce, je tu ohromná spojitost. Máme-li možnost výběru, mezi nasazením stovek vojáků, kteří jsou zranitelní, smrtelní a unavitelní, a nasazením pár osob, které sice jsou také zranitelní, smrtelní a unavitelní, ale také lépe ochranitelní, a máme-li prostředky pro možnost této volby, právě díky technice a technologiím, využijeme druhé možnosti.

2.5 Kyberterorismus a kybernetická kriminalita

Pod pojmem kybernetická kriminalita[5] je myšlena činnost založená na porušení zákona nebo ohrožení morálky společnosti. Jde o kriminalitu jako takovou, pouze s rozdílem jejího zprostředkování, a to v kyberprostoru. Tudíž jde o jakoukoliv protiprávní činnost, ať už o přestupek, trestný čin nebo jiný správní delikt.

Kybernetickou kriminalitou tedy je ohrožení, nebo narušení počítače a všeho kolem něj, to znamená, informací uvnitř počítače, programů, počítačových sítí a podobně.

Potrestání pachatele této kriminality je však složité, jakožto jedinec vykonávající fyzické protiprávní jednání, je osoba dohádatelná mnohem snadněji. Existují svědci, důkazy ve formě stop, které zanechá.

Dle trestního zákoníku jich může zanechat jedenáct druhů, a to daktyloskopické, trasologické, biologické, balistické, chemické, mechanoskopické, grafologické, pachové, věcné, mikroskopy a stopy paměťové. Zdaleka se nemusí objevit všechny u jednoho protiprávního jednání, ale podíváme-li se na kybernetickou kriminalitu, náš pohled se musí zúžit. Nevíme-li, odkud pachatel jedná, musíme vynechat daktyloskopické stopy. Trasologické stopy jsou pro nás bezvýznamné, nejspíše celou dobu sedí u počítače a chodí si maximálně pro stravu a na toaletu. Biologické stopy by přicházeli v úvahu, pouze pokud by se našlo „hnízdo“ pachatele, jinak jsou taktéž bezvýznamné. Balistické, chemické a mechanoskopické taktéž vynecháme, tato forma kriminality je fyzicky nenásilná. Grafologické stopy by se dali použít, dokáží-li se technici zpětnou vazbou dostat do pachatele počítače, styl písma nemusí být nutně ručně psaný. Pachové, věcné a mikroskopy jsou vyloučené, zrovna tak i paměťové.

Podíváme-li se na seznam druhů stop v souhrnu, vlastně jediné pouze teoreticky použitelné stopy jsou grafologické. Ty ovšem jsou samostatně minimálně použitelné.

Ovšem, pokud se dostaneme do pachatele počítače, již by se dala najít jeho poloha, pokud nevyužíval kaváren a podobných veřejných míst, kde se může společnost dostat do kyberprostoru v anonymitě, již se nám naskytují další možnosti stop.

[5] JIROVSKÝ, V. *Kybernetická kriminalita.* 1. vyd. Praha: Grada Publishing, a.s., 2007. s. 19 – 30. ISBN 978-80-247-1561-2.

Teoreticky, dostaneme-li se do kavárny, ve které byl, a budeme-li mít štěstí, dokážeme tam najít také jiné stopy.

Ale to jsou pouze domněnky a teorie. Praxe bývá mnohdy jiná. Pravdou však zůstává, že pachatel kybernetické kriminality bývá vždy o krok napřed.

Budeme-li chtít porovnat kybernetickou kriminalitu a kyberterorismus, je to jako bychom porovnávali protektorovanou pneumatiku a kvalitní pneumatiku na auto. Oboje má stejný význam, oboje je vyrobené ze stejného materiálu, avšak dopady v případě špatného výrobku jsou jiné. Zde ovšem nejde o výrobek, ale o následek jednání, za kterým bohužel tato činnost směřuje. Kyberterorismus má následky závažnější než kybernetická kriminalita, tedy, dá se velmi volně konstatovat, že jde v případě kybernetické kriminality o totéž jako u kyberterorismu, jen na menší cíle.

Oddělíme-li si od slova kyberterorismus slovo kyber a to samé uděláme i u kyber-kriminality, vzniknou nám dvě slova – terorismus a kriminalita. A můžeme na tato dvě slova užít definic běžně používaných.

Kybernetická kriminalita je vlastně taková, předzvěst kyberterorismu.

3. HROZBY KYBERTERORISMU

3.1 Co můžeme za kyberterorismus považovat?

, Dle Jirovského existují tři možnosti kyberterorismu, se kterými se plně ztotožňuji.

Jedná se o mediální terorismus, procesní terorismus a IT governance.

3.2 Mediální terorismus

Masmédia hýbají světem. Dovolují obrovskou manipulaci s lidmi. Naopak! Lidé dovolují obrovskou manipulaci sami se sebou prostřednictvím masmédií.

Zeptejme se dětí ze základní školy na reklamy. Garantuji Vám, že 99% z nich dovypráví nazpaměť většinu reklam. Zeptejme se maminek na mateřské dovolené a budou vědět všechno, co bylo v ranních, odpoledních nebo večerních zprávách. Například moji rodiče, nekomunikují se mnou po čas zpráv a můžu jim vyprávět cokoli. Jde ovšem pořád o zprávy? Tří minutová reportáž na téma „otevření nového butiku“, následuje další reportáž o veřejných záchodcích, taktéž tří minutová. V neposlední řadě musíme někomu udělit medaili za rekreaci a palec nahoru za sportovní výkon, případně palec dolů za trapas. Sledovanost neklesá, naopak! Vážnost a naplnění onoho významu „zprávy“ už ano. Pořád je řeč, ale, pouze o televizi. Vždyť ta má ovšem zpožděná data.

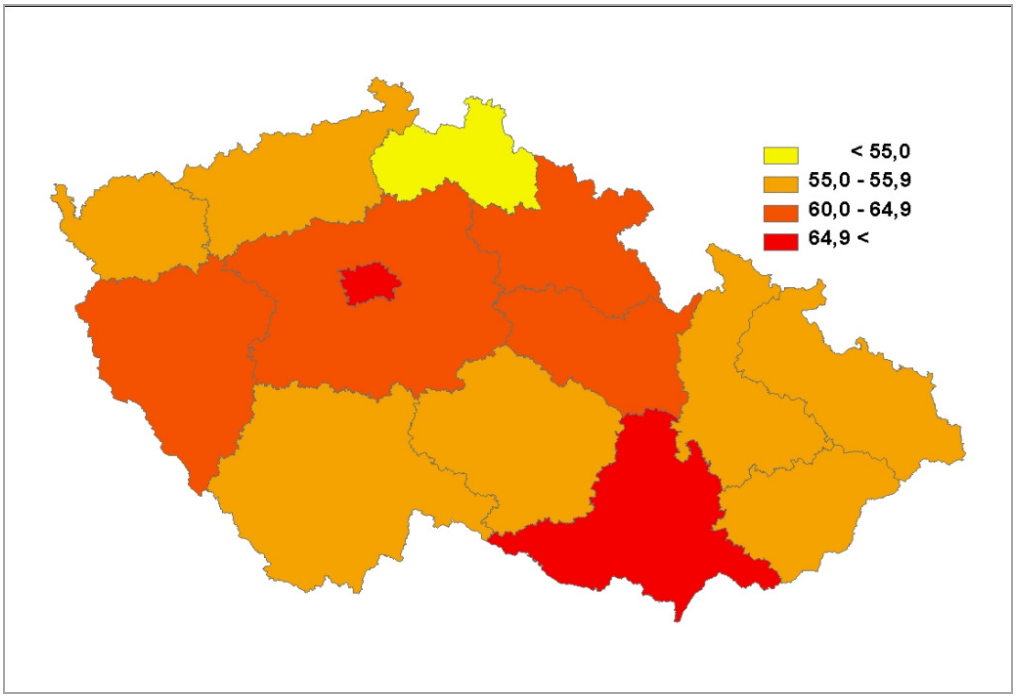
Papírová forma novin, dnes již spíše bulvární, než racionální.

Přesuneme se tedy - směr internet – ten do kategorie masmédií zapadá. Je rychlý, prostorově neomezený. Co je rychlé, bude jistě i pravdivé. Internetu se věří obecně více.[6]

Pro představu Český statistický úřad udělal studii, kde se zajímá právě o internet a ve výsledku své studie zveřejnil mapu České republiky ukazující na počet domácnostní (v procentech), které jsou připojené k internetu. Pro lepší simulaci využili dat z let 2010-2012.

[6] Dle mé analýzy formou jednoduchého dotazu v mém okolí.

Obrázek 4 Využití internetu v domácnostech v ČR



ZDROJ: Český statistický úřad[7]

Základní metody mediálního terorismu:[8]

- Internetové časopisy, noviny a bulváry. Co je na internetu, je pravda. Redaktoři těchto jistě důvěryhodných webových stránek taktně převedou čtenáře na stejný názor, jaký mají oni.
- Kybertronika. Téměř každý web, ve chvíli, kdy je otevřen, otevře i reklamu, pokud neotevře reklamu, jsou reklamy v tzv. banerech na něm. Tyto reklamy v sobě obsahují informace vnímané podprahově a tím pádem si čtenář ani neuvědomí, že něco takového viděl, ačkoliv mozek tuto zprávu zaregistroval.
- Provoz a rozšiřování webových stránek aktivistů s teroristickou aktivitou
- Aktivistický spam směřující k získání podpory pro svou stranu, program, dosažení cíle či jiné záměry.

[7] MANA, Martin. Využívání informačních a komunikačních technologií v domácnostech a mezi jednotlivci 2012. In:*Český statistický úřad* [online]. 2012 [cit. 2013-01-14]. Dostupné z: http://www.czso.cz/csu/2012edicniplan.nsf/p/9701-12

[8] JIROVSKÝ, V. *Kybernetická kriminalita.* 1. vyd. Praha: Grada Publishing, a.s., 2007. s. 144. ISBN 978-80-247-1561-2.

Tyto metody se často používají i ve volebních soubojích či jiných národních rozepřích, kde se část národa snaží získat druhou část na svou stranu.

3.3 Procesní terorismus

Podobně jako některé druhy terorismu se snaží procesní terorismus zničit prvky demokratického řešení sporů prostřednictvím demokracie. Mnohdy jde ruku v ruce s mediálním terorismem.

Procesní terorismus zneužívá zákonná ustanovení, nařízení, vyhlášky nebo pravidla či soudní moc k vyvolání soudních sporů. Tyto spory jsou nepochopitelné a výsledkem soudních řízení bývá omezení moci bezpečnostních sil a ozbrojených bezpečnostních sborů. Omezením moci bezpečnostních sil a ozbrojených bezpečnostních sborů se přímo úměrně omezí i bezpečnost daného státu. Druhým cílem útoku procesního terorismu je zatížení soudního systému státu, vyvolání masové nedůvěry v tu či onu stranu a díky tomu i zvyšování agrese obyvatel. V komplexu tedy opět hovoříme o ohrožení bezpečnosti státu.[9]

Spouštěcí mechanismus těchto sporů, naoko se dovolávajících lidských práv jsou nejčastěji nevládní organizace a sdružení. Lidská práva jsou dovolávána pouze hlasitě, tiše jsou zastřeny různé komerční, ekonomické nebo jiné kauzy. Bohužel vesměs vycházející kauzy.

3.4 IT governance

Zvýšením potřeby technologií se zvyšuje i potřeba správců technologií. Se zvýšeným počtem správců roste i jejich nenápadná moc.

IT governance je stav organizace, kdy se moc těchto správců dostane na takovou úroveň, kdy nenásilně a nenápadně ovládají rozhodující a řídící články organizace. Moc aktérů roste natolik, že se cíle organizací mění na cíle IT pracovníků. Ať už jsou sebevíce absurdní.

Typy vztahů v organizacích, dle ovlivnitelnosti rozhodování vztažených na IT[10]

[9] JIROVSKÝ, V. *Kybernetická kriminalita.* 1. vyd. Praha: Grada Publishing, a.s., 2007. s. 146. ISBN 978-80-247-1561-2.
[10] JIROVSKÝ, V. *Kybernetická kriminalita.* 1. vyd. Praha: Grada Publishing, a.s., 2007. s. 147. ISBN 978-80-247-1561-2.

- Obchodní monarchie značí, že rozhodování v organizaci má jednotlivec, nebo pár jednotlivců, vesměs z managementu obchodních složek organizace. V této fázi nemají IT pracovníci žádnou moc při rozhodování.
- IT monarchie je pravým opakem obchodní monarchie. Počet pracovníků, kteří rozhodují je zachován. Mění se pouze postava rozhodujícího, z managementu obchodních složek na IT pracovníky.
- Feudalismus znamená, že rozhodování je v režii vedoucích pracovníků.
- Duopolie. Organizace je rozdělena na dvě části. První část je založena na požadavky IT pracovníků a je z nich vesměs i složena a druhá část pojímá ostatní orgány organizace.
- Federální uspořádání. V tomto případě nejvyšší orgán organizace pojímá zástupce odboru nebo části organizace s určitými pravomocemi.
- Anarchie. Vysvětlení je jasné. Nikdo neposlouchá nikoho, všichni dělají, co chtějí.

V každém případě se jedná o velmi promyšlený, neviditelný nátlak, který existuje pouze díky hrozbám. Výhodou IT pracovníků je, že si téměř vždy dokáží nalézt důvod. Díky odůvodnění jejich činů a požadavků, mohou docílit vlastních požadavků, které jsou zaobaleny do těch předkládaných.

3.5 Druhy cílů

Vyjmenovat všechny hrozby, které s sebou nese kyberterorismus je nemožné. Každým dnem, každou hodinou i každou minutou vznikají nové a nové metody a způsoby útoků, na které není ochrana.

3.5.1 Obecně

Cíle kyberteroristických útočníků mohou, jsou a budou rozmanité. Jakož je každý terorista něčím osobitý, stejně tak bude osobitý i kyberteroristický útok. V této podkapitole byla snaha o vytvoření určité struktury možných cílů kyberteroristických útoků. Nelze vymezit všechny cíle, avšak většina jich tu vypsaná bude.

- Kritická infrastruktura

- Doprava (dopravní sítě, komplexy dopravních zařízení, atd.)
- Energie (voda, plyn, elektřina, ropa, energovody, atd.)
- Zdravotnictví
- Finanční systém, ekonomika (informace o bankovních účtech nebo platebních kartách a manipulace s nimi, atd.)
- Mobilní operátoři (kolapsy signálů, informace o majitelích telefonních čísel, nabourávání se do telefonů uživatelům, odposlouchávání atd.)
- Ochranné systémy státu (technické dokumentace, plány, seznamy, atd.)
- Útočné systémy státu (technické dokumentace, plány, seznamy, atd.)
- Vládní úřady (státní tajemství, státní ekonomika, atd.)
- Vývoj IT (softwarové chyby, zdrojové kódy softwaru, atd.)

3.5.2 Další možný pohled[11]

V budoucnu se může se jednat například o:

- Infrastrukturu bankovních a finančních institucí
- Hlasové komunikační služby
- Elektrické rozvodné sítě
- Infrastrukturu ropného průmyslu
- Zdroje vody a vodní díla

[11] JIROVSKÝ, V. *Kybernetická kriminalita.* 1. vyd. Praha: Grada Publishing, a.s., 2007. s. 148. ISBN 978-80-247-1561-2.

3.6 Jak hrozbám předcházet?

Perfektní připravenost. Skládající se minimálně ze špičky TOP IT pracovníků s dokonalými znalostmi a ze špičky dostupných technologií.

Hlavní pomocí, která světu může být dána, je nepodceňování dané situace. Každý čin, který je podceňován, končívá fiaskem. Vždy je lepší, být připraveni, aneb kdo je připraven, není překvapen.

Bezpečnost je v této situaci na prvním místě, bude-li bezpečnost počítačů, počítačových sítí a informací uvnitř na nejvyšší úrovni, stále vylepšovaná, riziko napadení bude nízké.

V civilní sféře, lze hrozbám předcházet, nebo alespoň snížit riziko, programy zabezpečujícími software a jejich pravidelnými aktualizacemi, zabezpečením používané sítě a rozumného a odpovědného chování při používání sítě.

Na internetu, tedy, taktéž v kyberprostoru, se nachází webová stránka zabývající se protiteroristickými aktivitami. Stránka je pravidelně aktualizovaná a důvěryhodná.

4. ÚTOČNÍK „KYBERTERORISTA“

Kyberterorismus by neexistoval, kdyby neexistoval kyberprostor, ale hlavně by neexistoval, kdyby neexistovali útočníci kyberterorismu, tak zvaní kyberteroristé.

V této kapitole rozlišíme několik druhů kyberteroristů.

4.1 Osoba útočníka

Osobu kyberteroristy rozhodně nepoznáme na ulici. Kyberteroristickým útočníkem může být kdokoli, učitelka ve školce, IT-technik v bance, prodavač v obchodě nebo žák základní školy. Vzhledově se nemusí nijak lišit. Rozhodně si nemůžeme kyberteroristu představovat jako brýlatého, vyvrtlého muže vyšší postavy, ve středních letech s kulatými brýlemi, neupraveného a s kabely okolo těla.

Obrázek 5 Kyberterorista

ZDROJ: How to keep your computer safe from hackers. In: *ContactPointe* [online]. 2011 [cit. 2013-03-04]. Dostupné z: http://blog.contactpointe.com/2011/06/how-to-keep-your-computer-safe-from-hackers-other-online-threats/

4.2 První možný pohled

Rozdělíme-li si kyberteroristy do skupin, získáme jich několik. Jako první možnost jsou teroristické skupiny jako takové. Za druhou možnost kyberteroristy můžeme považovat jednotlivé osoby, které mohou být jak kyberteroristy, nebo pouze pachateli kybernetické kriminality. Další, tedy třetí, možností, může být, dle mého názoru stát, je otázkou, zda ještě pořád půjde o kyberterorismus, nebo o kybernetickou válku.

4.2.1 Teroristické skupiny

V této skupině se nachází většina teroristických skupin, které známe. Nikdo nemůže zapřít existující riziko, že se tito teroristé neprojeví i v kyberprostoru. Někteří se již projevili, nemusí to být již dokonaným útokem, postačují i prezentace, webové stránky, různé skupiny na sociálních sítích, podporující právě hnutí té či oné teroristické skupiny.

Napíšeme-li do vyhledávače sociální sítě Facebook název jakékoliv známější teroristické skupiny, odpovědí na vyhledávání bude a je několik desítek výsledků, které podporuje na tisíce uživatelů. Některé více, některé méně.

Al-Káida například začala vydávat online časopis v anglickém jazyce, kde sdílí své myšlenky, verbuje další příznivce a dává jim další potřebné informace.[12]

4.2.2 Jednotlivci

Budeme-li se bavit s pěti lidmi, všichni nám řeknou jiný názor na otázku, zda se za útočníka kyberterorismu dá považovat i jednotlivec.

Existuje nespočet jedinců, kteří sedí v křesle u počítače a snaží se dostat do e-mailu svého kamaráda, kolegy nebo nadřízeného. Dá se takové jednání považovat za kyberterorismus? Budeme-li vycházet v definice kyberterorismu, dle D. E. Denning, tak nikoli. Jedná-li se, ale, o jedince, který svůj útok směřuje proti politickému systému nebo jiné oblasti kritické infrastruktury, již se o kyberteroristu jedná. V opačných

[12] http://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies online 2.3.2013

případech můžeme mluvit o hackingu, kybernetickém výpalném, šíření materiálů se závadným obsahem, sparingu, warezu, crackingu, sniffingu nebo cybersquattingu[13].

Má-li útočit teroristická skupina, zmíněná výše, útočí tak i tak prostřednictvím jednotlivce. Ten buď je součástí skupiny, nebo není.

Bude-li vycvičen terorista v teroristickém výcvikovém středisku, bude vycvičen ve fyzickém útoku, v bombovém útoku, ale v mizivém procentu v kybernetickém útoku. Na to si seženou jiné. Jednak jsou tací, kteří jsou vycvičeni mnohem lépe a díky tomu mohou cvičit jiné, a jednak, když nemusí jiné cvičit, mohou tyto útoky zkombinovat.

4.2.3 Stát

Stát jakožto organizace, se bude snažit vždy vyčnívat nad okolními státy. Bude chtít být lepší, připravenější a odhodlanější. A využije k tomu všeho dostupného. I možné špionáže do soukromí ostatních států, do jejich tajemství a duševního vlastnictví, pomůže-li jim to být lepší, zjistit jejich vojenské taktiky útoku i obrany, nové vědecké výzkumy a plánované změny v zákonech. Všechno tohle a mnohem více, může přispět k vyřešení mezinárodních vztahů, sic protizákonně a nečestně, ale může.

Tyto útoky, aby šlo o kybernetický terorismus provedený státem, musí být vždy státem iniciovány. Jde tedy o určité složky vlády, nebo organizace s vládou spjaté.

Výše jsme si představili útok státu vůči jinému, existuje ovšem další možnost. Útočí-li stát směrem ven, může útočit i směrem dovnitř. Je to nelogické, i logické. Představme si situaci, na které by tento útok mohl být lépe pochopitelný. Učitelé na škole nemají takovou důvěru a takový respekt, jaký by si představovali. Tak nezištně budují překážky žákům do cesty. Žáci reagují vyhledáváním pomoci, kde jinde, než u učitelů. Ti si tím vybudují určitou důvěru, kterou potřebují.

Převedeme-li tuto situaci zpět na stát, tedy, zakomponujeme definici kyberterorismu, s kterou pracujeme, znamená to pro nás zastrašení nebo donucení obyvatel k vykonání nebo naklonění se té či oné politické strategii, vykonané prostřednictvím kyberprostoru.

[13] JIROVSKÝ, V. *Kybernetická kriminalita.* 1. vyd. Praha: Grada Publishing, a.s., 2007. s. 102 - 107. ISBN 978-80-247-1561-2.

4.3 Druhý možný pohled

Toto dělení je zaměřeno hlavně na motivaci útočníků. Motivace existuje různá, může jít o pomstu, peněžního zisku, zisku určitých více či méně důležitých dat nebo jen snahu o zviditelnění.

Jedná se o hackera, frustrovanou osobu, osobu bažící po pěnězích a datech a politického aktivistu. Níže budou tyto osoby rozvedeny.[14]

4.3.1 Hacker

Tato osoba nemusí mít téměř žádnou motivaci. Může jít vlastně o zábavu. V osobě hackera můžeme spatřovat osobu bez vzdělání v oboru, nebo naopak o osobu, jenž je v oboru specialistou. Vzdělání se odráží v dosaženém cíly, od obyčejného získání přístupového hesla e-mailu spolužáka až například ovládnutí finančního systému.

Kyberprostor nabízí takovýmto jedincům dostatečné množství příruček a programů ukazujících jak toho či onoho cíle dosáhnout.

Cílem hackera bývá většinou spíše zviditelnění se, než ublížení postiženému útokem. Pokud je hacker součástí hackerské komunity, jde o získání určitého postavení a obdivu, tedy, čím zabezpečenější systém naboura, tím lepší je.

[14] Černý Michal. Kyberterorismus v informační společnosti. Část II. Inflow: informatik journal [online] 2012 [citace 2013-03-04]. Dostupný z WWW: http://www.inflow.cz/kyberterorismus-v-informacni-spolecnosti-cast-ii. ISSN 1802-9736

Hackeři dodržují pravidla, čímž se liší od jiných útočníků, kteří útočí-li, útočí s určitou motivací, nikoli pro zábavu nebo získání obdivu, apod. Mezi tato pravidla se řadí:[15]

1. Počítačové technologie musí být přístupné všem a zdarma.
2. Veškeré informace jsou a musí být zdarma.
3. Absolutní nedůvěra ve vládu a podobné mocenské autority.
4. Posuzování hackerů musí být na základě jejich schopností a dovedností.
5. Počítač může sloužit i umění a kráse.
6. Skrz počítač může být život lepší.
7. Zákaz poškozování systémů.
8. Zákaz vstupování do státních počítačů.

4.3.2 Frustrovaná osoba

Tato osoba může být osobou nedoceněnou, bývalým zaměstnancem, nedoceněným programátorem, apod.

Motivem není, jako v předchozí podkapitole, zviditelnění se nebo obdiv, vesměs jde hlavně o pomstu, nevyřešený problém.

Velice často se jedná o tzv. „vnitřního nepřítele“, frustrovaná osoba napadá systém z vnitřku. Uvědomuje-li si jedinec, že se děje něco, co považuje za útok proti své osobě, buduje základy svého útoku již v raném období, kdy ještě není situace vyhrocená a on má do systému legální přístup. V případě vyhrocení situace, má možnost okamžitého útoku.

Konečná fáze nepřináší útočníkovi žádné výhody či zisky, ale pocit uspokojení. Naopak pro napadeného znamená tento útok obrovské ztráty.

[15] JIROVSKÝ, V. *Kybernetická kriminalita.* 1. vyd. Praha: Grada Publishing, a.s., 2007. s. 52 - 56. ISBN 978-80-247-1561-2.

4.3.3 Osoba bažící po penězích a datech

Jde o zloděje, kybernetické útočníky a specialisty.

Motivací těchto osob je zisk, ať už finanční nebo ve formě dat. Z větší části pravděpodobnosti těchto útoků nepůjde o malé finanční obnosy, příp. množství dat, naopak budou velkých rozměrů.

Útoky jsou tiché, bez upozorňování a snahy o zviditelnění, vesměs bezchybné. Čím méně nápadné jsou útoky, tím lépe.

Bránit se osobám bažícím po penězích a datech je velmi obtížné, už jen z důvodu jejich znalostí a schopností uvést tyto znalosti do praxe.

4.3.4 Politický aktivista

Politickému aktivistovi nejde o pomstu nebo peníze či data. Jeho cílem je mediální ohlas, co největší obdiv. Největší odměnou pro takovou osobu by bylo, kdyby z ní udělali hrdinu.

Snaha politického aktivisty se vždy odráží od politické situace okolo něj. Nikde není dáno, jakým způsobem útočí, může útočit jako výše uvedení útočníci, nebo může přímo napadat státní systémy.

4.4 Příklad útočníka

Příkladem nám může být skupina Anonymous. Tuto skupinu nemůžeme zařadit ani dle prvního či druhého pohledu na osobu útočníka. Nejčastěji jsou členové Anonymous zařazování mezi hackery, ale setkáváme se i s označením teroristické skupiny, nebo politických aktivistů. Neútočí totiž pouze na určité cíle, které by měli společné rysy. Jejich útoky směřují i na zdánlivě, nebo opravdu, cizí společnosti nebo podnikatele, kteří s aktivitou Anonymous nemají pranic společného.

Obrázek 6 Anonymous

ZDROJ: My jsme Anonymous. In: *Evropský rozhled* [online]. 2010 [cit. 2013-03-04]. Dostupné z: http://www.evropsky-rozhled.eu/my-jsme-anonymous/

Skupina Anonymou[16]s je známá od roku 2003, pod kůži se lidem dostala však teprve v roce 2011. Jsou zde jasně viditelná hackerská pravidla – chybí hierarchie, vytyčené cíle a je velmi obtížné zařazení jednotlivce. Ti se sice k této skupině hlásí, ale chybí jasné důkazy o jejich členství.

Síla skupiny Anonymous je hlavně v množství členů, když bude odhalen jeden člen, pro skupinu jako takovou půjde o nepocítitelný čin. Naopak ve chvíli, kdy se členové spojí a zaútočí společně, má útok sílu neuvěřitelných rozměrů a hlavně je špatně dohádatelný, jelikož směřuje z velkého množství pozic a míst. Množství jejich útoků je také velmi nejasné, k řadě útoků se nehlásí, ale vše nasvědčuje tomu, že jsou útočníky právě oni.

Členové Anonymous útočí pomocí DDoS útoků. DDoS útoky budou vysvětleny níže.

Mezi příklady jejich útoků se řadí například Projekt Chanology v roce 2008, kde byl útok směřován proti scientologické církvi, cílem mělo být upozornění na cenzuru internetu a názor scientologické církve na internet. Jako další příklad je možné poukázat

[16] Černý Michal. Kyberterorismus v informační společnosti. Část II. Inflow: informatik journal [online] 2012 [citace 2013-03-04]. Dostupný z WWW: http://www.inflow.cz/kyberterorismus-v-informacni-spolecnosti-cast-ii. ISSN 1802-9736

na Operaci Payback v roce 2010, která byla směřována proti Visa a MasterCard International, kteří odmítli sponzorovat projekt Wikileaks. Jejich weby byly díky útokům Anonymous nedostupné.

4.5 Důvody útoku

Důvody kybernetických útoků mohou být jakékoli. Opět na tuto kapitolu použijeme druhy terorismu, za které se obecně považují politický terorismus, náboženský terorismus, kriminální terorismus a psychotický terorismus (viz. kapitola 2.1 Kyberterorismus jako součást terorismu). Jde o rozdělení terorismu, tím pádem by dalším druhem terorismu měl být kyberterorismus. Budeme-li se snažit rozkrýt důvody kyberteroristických útoků, použijeme právě výše uvedené druhy.

Politický kyberterorismus. Za tento druh kyberterorismu se dají považovat všechny kybernetické útoky, opírající se o politický systém. Ať už mluvíme o státním kyberterorismu směrem ven i dovnitř. Vždy za těmito útoky bude stát politický záměr.

Náboženský kyberterorismus. Islámští teroristé jsou ochotni navléci na své tělo vestu plnou výbušnin a uprostřed nákupního centra stisknout spoušť. Důvody jejich činů řešit nebudeme, zaprvé by se tato práce začala stáčet jiným směrem a zadruhé nevíme, jaká je druhá strana mince. Všichni vidíme stranu mince, kterou hlásá Amerika – dělají tyto činy dobrovolně a za Alláha. Ale kdo ví, zda to není právě proto, že jim američtí vojáci vzali všechno, co měli a oni se chtějí pomstít? Přišli o celou rodinu, viděli tolik, že by byli radši slepí a je to jediná možnost, kterou jim život nabízí. Nyní, ale odbočujeme od tématu. Závěrem k náboženskému kyberterorismu, důvodem je jak z názvu vidno, náboženství. Může být jakékoli, nikde není dáno, že křesťan nemůže být teroristou, ani kyberteroristou. Ba naopak, pod svícnem bývá tma, a mluví se pouze o východních náboženstvích.

Kriminální kyberterorismus označuje organizovaný zločin prostřednictvím kyberprostoru, jejich úsilí směřuje vesměs na civilní obyvatelstvo.

Psychotický kyberterorismus. Abychom si více přiblížili popis takového útoku a útočníka, použijeme opět jiné přirovnání – chovají se, jako když dítěti vezmete hračku. Tyto útoky nemusí mít žádný vážný důvod, útočníci, vesměs nebývají psychicky v pořádku, a pokud se rozhodnou, vyberou si pouze cíl. Cílem může být cokoli, kdokoli.

Kolikrát postačuje, že se daný útočník dostane do masmédií. Pro něj je výhra, již se nedívá na dopady, které jeho útok měl. Že výpadek kritické infrastruktury nemocnice zabil stovky lidí.

4.6 Druhy útoků

Stanislav Kužel je bývalý šéfredaktor magazínu Proffesional Computing a Software Developer. Sepsal elektronickou knihu Kybernetická kriminalita: Od hackerů ke kybernetickým válkám.

V této knize popisuje vše ohledně kybernetické kriminality, kybernetických válek a kyberterorismu, mezi nimi i druhy útoků kyberteroristů.[17]

V této podkapitole se budeme zabývat pouze druhým směrem útoků, tím, který je nebezpečnější a důraznější, a to útokem, jenž přímo napadá konkrétní informační síť nebo ji likviduje.

V tomto směru útoku definuje několik úrovní:

- Řízení sympatizantů a podobných lidských „zdrojů“ – zde poukazuje na využívání informačních technologií k řízení lidí v teroristických skupinách. Možnému rozšíření působení na celý svět, díky nepřetržitému kontaktu prostřednictvím kyberprostoru. V tomto směru taktéž předávání informací a úkolů členům
- Lokální kyberútok – je tím myšlen již přímý útok na danou technologii, nebezpečnost útoku je přímo úměrná zkušenostem, vybavenosti a připravenosti teroristické skupiny, stejně jako jejím cílům.
- Souběžný útok – jedná se o několik útoků v různých úrovních zároveň. Při souběžném útoku jde buď o přípravu na likvidaci daného cíle, likvidaci daného cíle nebo o totální dezorientaci a kolaps, zakončený fyzickými napadeními.

[17] STANISLAV KUŽEL. *Kybernetická kriminalita: Od hackerů ke kybernetickým válkám* [online]. Bispiral, s.r.o., 2012 [cit. 2013-03-01]. BusinessIT ebooks. Dostupné z: http://www.businessit.cz/ebooks/kyberkriminalita.pdf

4.6.1 Rozdělení útoků

- DDoS útoky[18]. Tyto útoky jsou velmi jednoduché. A jak se říká, v jednoduchosti je síla, nejen díky tomuto rčení jsou také velmi účinné. Podstatou těchto útoků je zahlcení serveru, na který je útok prováděn. Serveru jsou kladeny dotazy s IP adresou, na které musí server odpovědět. Proti tomuto druhu útoku je těžká obrana, díky koordinovanému útoku a velkému množství IP adres podílejících se na něm. Pokud je útok proveden správně, stane se stránka nedostupnou.
- Kořenové DNS servery. Ty převádí doménový tvar adresy na IP adresu. Pokud je útok směřován na DNS servery. Tento útok není ani tak nebezpečný, jako spíše nepohodlný. Na uživatele je kladen poté větší nátlak, je myšlen v tom směru, že by si museli pamatovat IP adresy, aby se na servery mohli dostat. DNS servery jsou označeny písmeny „A“ až „M“. Pro dokonalost útoku by musel útočník vyřadit všech třináct serverů, což je zdlouhavé. Výsledkem by byl ovšem nefunkční internet. DNS servery, laicky řečeno, drží internet pohromadě. Naštěstí jsou poměrně chráněné.

4.7 Metody útoků

Co útok, to metoda. Tak se dá shrnout počet možných metod útočníků. Nedá se říci, že všechny útoky jsou na úrovni kyberterorismu, ale s trochou snahy útočníka se dají ke kyberteroristickými útokům použít.

Cybersquatting. Jedná se o registrování domén, které mohou být lehce zaměnitelné s doménami důležitými. Od internetových vyhledávačů, institucí, organizací a podniků po domény velkých osobností.

Kybernetická šikana. Cíl je z názvu patrný. Poškození či ublížení určité osobě. Může být ve formách uveřejnění jejích osobních údajů, soukromých dokumentů či osočujících, nepravdivých textů.

Cracking. Aneb útok zvenku.

[18] Černý Michal. Kyberterorismus v informační společnosti. Část I. Inflow: informatik journal [online] 2012 [citace 2013-03-04]. Dostupný z WWW: http://www.inflow.cz/kyberterorismus-v-informacni-spolecnosti-cast-i. ISSN 1802-9736

Hacking. Viz. podkapitola 4.3.1. Hacker.

Phishing, Útočník získává určité informace tím, že se fiktivně vydává za určitou existující společnost. Jasným příkladem jsou v masmédiích velmi často zmiňované e-maily vyžadující hesla od e-mailů, bankovních účtů či vlastních serverů.

Pharming. Je velmi podobný phishingu, s tím rozdílem, že hesla nejsou od majitelů vyžadována, avšak nenásilně získávána skrz podvodné domény.

Social engineering. Jde o další velmi účinnou metodu útoku. Kde se útočník snaží přesvědčit uživatele, aby sám narušil systém a jeho ochranná opatření. Například viry zdánlivě vypadající jako zábavné prezentace, videa či GIF obrázky.

Spamming. Jde o zahlcení e-mailových a jiných schránek nevyžádanou poštou, reklamou apod. Na čím více domenách je osoba registrovaná, tím více spamů jí do schránky přijde. Stejně tak, čím déle je e-mailová schránka zaregistrována, tím více spamu je tam zasíláno. V konečné fázi se dá říci, že denní přísun elektronické pošty činní více jak z poloviny spam.

Adware. Systematické získávání dat a často i odposlechu z koncových stanic. Znepříjemňující vesměs reklamní činností, vyskakujícími pop-up okny nebo bannery.

Spyware. Získává informace o konkrétním uživateli. Software se může sám nainstalovat do počítače, bez vědomí uživatele. A sám, opět, bez vědomí uživatele, odesílá i jejich data.

Viry. Ničí nebo poškozují daný software, hardware nebo prvek.

Trojské koně. Škodlivý software zdánlivě se tvářící jako dobrý, užitečný program. Tento program kolikrát opravdu užitečný je, má však i další funkce, které uživatel nevidí. A to například odposlech, zasílání zpráv, hesel.

Sniffing. Tato metoda odposlouchává pakety. Pracuje-li paket s nešifrovanou komunikací, je zde větší pravděpodobnost útoku, než u pakety pracujícího se zašifrovanou komunikací.

Spoofing. Útok založený na falešné imunitě. Existuje zde reálná možnost propojení s metodou sniffingu, kdy se získané informace zasílají ještě třetím stranám.

DoS. Jde o formu útoku, kdy se server naschvál zahtí falešnými požadavky na poskytnutí konkrétních informací, služby, apod. S postupem času se DoS metody přesunuly a využívají se více DDoS metody, změna vyvstává s počtu počítačů zajišťujících útok.

Bombing. Nejméně nebezpečná metoda útoku. Lokální síť je zahlcována pakety. Ovšem pouze lokální síť.

MiM. Metoda konkrétního útoku, nikoli obecného. Jedná se o útok na dva uzly a jejich vzájemnou komunikaci.

Možností útoků je více, než které tu jsou uvedené. Existují různá propojení metod, jejich kombinace. V této době hojně využívané.

4.8 Příklad určitého útoku

Tzv. Stuxnet 1.0. objevený v roce 2010 nebo 2007 anebo nakonec 2005? Donedávna bylo všem jasné, že byl objeven v roce 2010 a vytvořen v roce 2009. Dle nejnovějších výzkumů firmy Symantec byl tento malware používaný již v roce 2007. Nepřímé důkazy ukazují již na rok 2005.[19]

K pojmu SCADA systém[20], nebo-li „Supervisory Control And Data Acquisition (operátorské řízení a sběr dat). Tento systém byl poprvé použit v roce 1960. Jde o počítačový systém shromažďující a analyzující data v reálném čase. Vesměs je používán jako monitorování a ovládání zařízení v telekomunikacích, energetických odvětvích, dopravě, apod.

Obrázek 7 Stuxnet

ZDROJ: US, Israel or Russia, who is Behind Stuxnet?. In: *The hacker News* [online]. 2011 [cit. 2013-03-04]. Dostupné z: http://thehackernews.com/2011/12/us-israel-or-russia-who-is-behind.html

[19] Nové důkazy: Stuxnet fungoval minimálně od roku 2007. In: CONSTANTIN, L. a P. KREUZIGER. *Businessworld* [online]. QuinStreet Inc., 2013 [cit. 2013-03-04]. Dostupné z: http://businessworld.cz/novinky/nove-dukazy-stuxnet-fungoval-minimalne-od-roku-2007-10505

[20] What is SCADA?. In: *Webopedia* [online]. 2013 [cit. 2013-02-12]. Dostupné z: http://www.webopedia.com/TERM/S/SCADA.html

Cílem Stuxnetu byl íránský Siemens S7-417 controller v nukleárním centru Busherh a Siemens S7-315 controller v íránském Natanzu, v centru Centrifuge operation.[21]

Během jednoho roku napadl tento malware na 100000 počítačů.

Díky novým výsledkům výzkumu bylo zjištěno, že do íránského Natanzu nedorazil Stuxnet 1.0, ale Stuxnet 0.5. Tento „starší" model napadá software Step 7.

Software Step 7 je používán k programování logických ovladačů. Pro přiblížení, jde o digitální počítače ovládající chod průmyslových strojů a procesů. Tím pádem by majitelé Stuxnetu 0.5 mohli ovládat ventily, které plnili centrifugy na obohacování uranu UF6. Dopady by mohly být obrovské. Zničení systému centrifug a i celého komplexu.

Nástupcem Stuxnetu 0.5 byl známější Stuxnet 1.0. Ten fungoval na stejném principu, s tím rozdílem, že zasahoval jiné programy logických ovladačů, které kontrolovaly rychlost otáčení centrifug na obohacování uranu UF6. Stuxnet 1.0 se oproti svému předchůdci šířil nejen přes USB flash disky, ale šířil se i místními sítěmi. Využíval k tomu zero-day zranitelnost operačního systému Windows.

U zero-day útoků jde o nalezení slabiny, která může být odstraněna až následnou aktualizací a opravou. Uvědomíme-li si, kolik uživatelů aktualizace vůbec nestahuje, je to velmi příhodná šance například právě pro Stuxnet.

Stále se ovšem neví, kdo za vytvořením viru stojí. Co se ovšem ví, je skutečnost, že jde o první virus, který je schopný dosáhnout neuvěřitelných následků, včetně dopadů na životech.

[21] STANISLAV KUŽEL. *Kybernetická kriminalita: Od hackerů ke kybernetickým válkám* [online]. Bispiral, s.r.o., 2012 [cit. 2013-02-12]. BusinessIT ebooks. Dostupné z: http://www.businessit.cz/ebooks/kyberkriminalita.pdf

5. ANALÝZA INFORMOVANOSTI OBYVATEL O KYBERTERORISMU – DOTAZNÍK

5.1 Vyhodnocení dotazníku

Pro lepší přehled o informovanosti obyvatel o kyberterorismu je zde šetření mezi lidmi formou dotazníku.

Bylo dotázáno šestnáct respondentů, kteří vyplnili krátký dotazník (viz Přílohy). Respondenti byli různých věkových kategorií a různých profesí, od studentů, přes podnikatele po zaměstnance.

Respondenti zodpověděli sedm otázek. Jmenovitě otázky zněly – pojem kyberterorismu, důvod kyberteroristických útoků, počátek kyberterorismu, zda by poznali kyberteroristu podle vzhledu, zda existuje hrozba kyberterorismu v České republice, počet kyberteroristických útoků a možnost zamezení dopadů kyberteroristických útoků. Níže rozpracujeme veškeré otázky a shrnuté odpovědi respondentů.

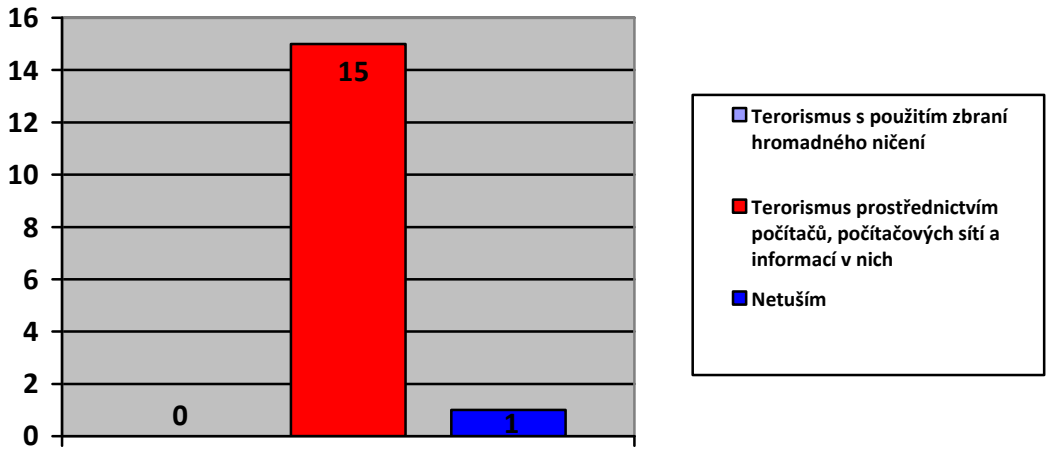
Věkové kategorie respondentů se pohybovaly od 18 let. Kategorií bylo pět (do 18 let, 19 – 29 let, 30 – 45 let, 46 – 55 let a více než 55 let) V první kategorii byli dotázáni 4 respondenti, v další kategorii taktéž. Po třech respondentech bylo v kategoriích 30 – 45 let a 46 – 55 let. V poslední kategorii, nad 55 let, se nachází dva respondenti.

5.2 Co si představíte pod pojmem kyberterorismus?

První otázka v dotazníku. Respondenti měli na výběr ze tří možností, první možností bylo, že jde o terorismus s použitím zbraní hromadného ničení, druhou možností byl terorismus prostřednictvím počítačů, počítačových sítí a informací v nich a jako třetí možnost bylo „netuším“.

Patnáct z šestnácti respondentů si myslí, že jde o terorismus prostřednictvím počítačů, počítačových sítí a informací v nich.

Pouze jeden respondent neví, co si pod tímto pojmem má představit. Vzhledem k vysokému věku respondenta, je to zcela pochopitelné. S tímto dotazníkem se dále pracovat nebude. Počet respondentů se tedy na další otázky snižuje na patnáct.



Graf 1 Co si představíte pod pojmem kyberterorismus?

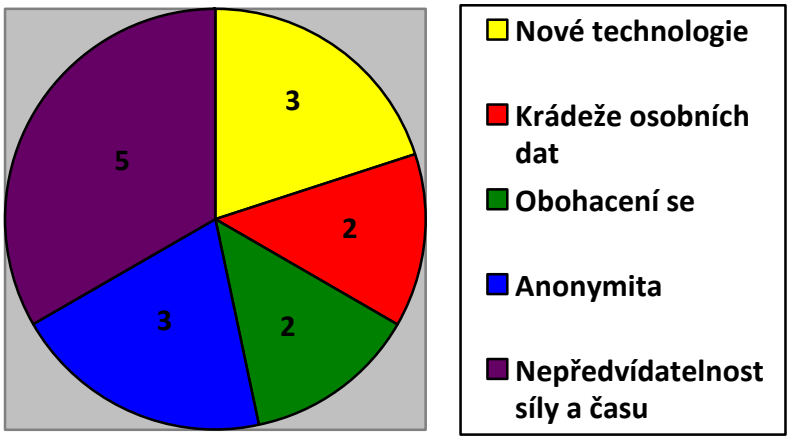
5.3 Co si myslíte, že je důvodem kyberterorismu?

V této otázce dostali respondenti na výběr z šesti odpovědí. Odpovědi zněly následovně: nové technologie, krádeže osobních dat, obohacení se, anonymita, nepředvídatelnost síly a času útoku a jako poslední možnost byla kolonka „jiné“ s prostorem na doplnění. Poslední kolonky nevyužil žádný respondent.

Jeden respondent mne upozornil, že je na povážení, zda tato druhá otázka má být důvodem, nebo cílem. Ovšem chceme-li dosáhnout určitého cíle, musíme k tomu mít důvod.

Zde již odpovědi byly rozmanitější.

Tři respondenti byli přesvědčeni o první možnosti a to, že důvodem kyberterorismu jsou nové technologie. Dva další respondenti mají pod důvodem kyberterorismu skryté krádeže osobních dat. Dvakrát respondenti zvolili za důvod kyberterorismu obohacení se. Tři respondenti poté anonymitu. Jako poslední možnost a to nepředvídatelnost síly a času útoku označilo nejvíce respondentů, přesněji pět.



Graf 2 Důvod kyberteroristických útoků

5.4 Víte, kdy začalo období kyberterorismu?

Ve třetí otázce byli respondenti dotázáni na počátek období kyberterorismu, s možnostmi odpovědí: V devatenáctém, dvacátém nebo jednadvacátém století.

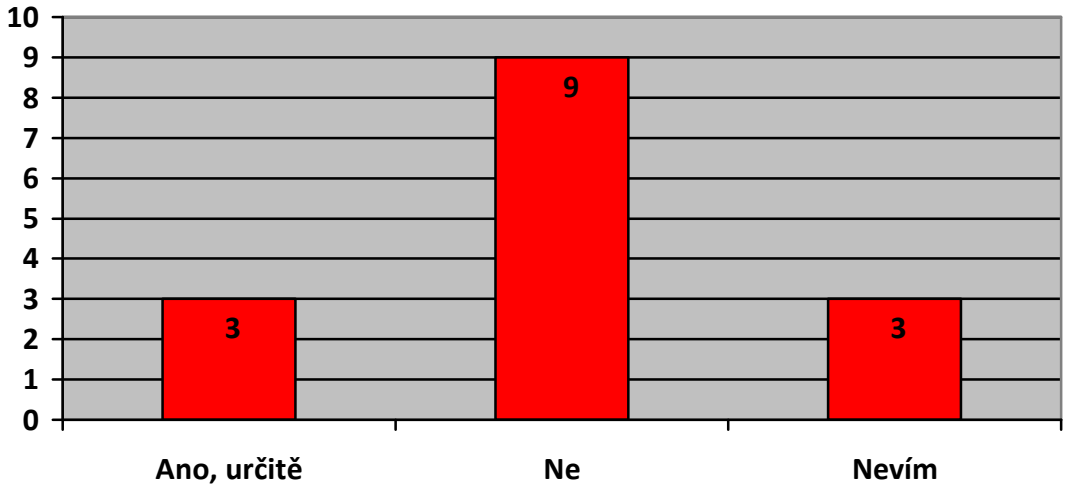
Devatenácté století nezvolil žádný respondent. Další dvě možnosti byly téměř nastejno odpověďmi. Osm respondentů si myslí, že ve dvacátém století a zbylých sedm respondentů se uchýlilo k jednadvacátému století.

Graf 3 Počátek kyberterorismu

5.5 Poznal/a byste kyberteroristu podle vzhledu?

Čtvrtá otázka se dotazovala na vzhled kyberteroristy. Zda si respondenti myslí, že by poznali kyberteroristu, kdyby proti nim šel například na ulici.

Tři respondenti si myslí, že ano. Devět respondentů si je jistých, že kyberteroristou může být vzhledově jak upravený mladý muž v obleku, tak žena oblečená, s nadsázkou, do jutového pytle. Další tři respondenti si nejsou jistí.

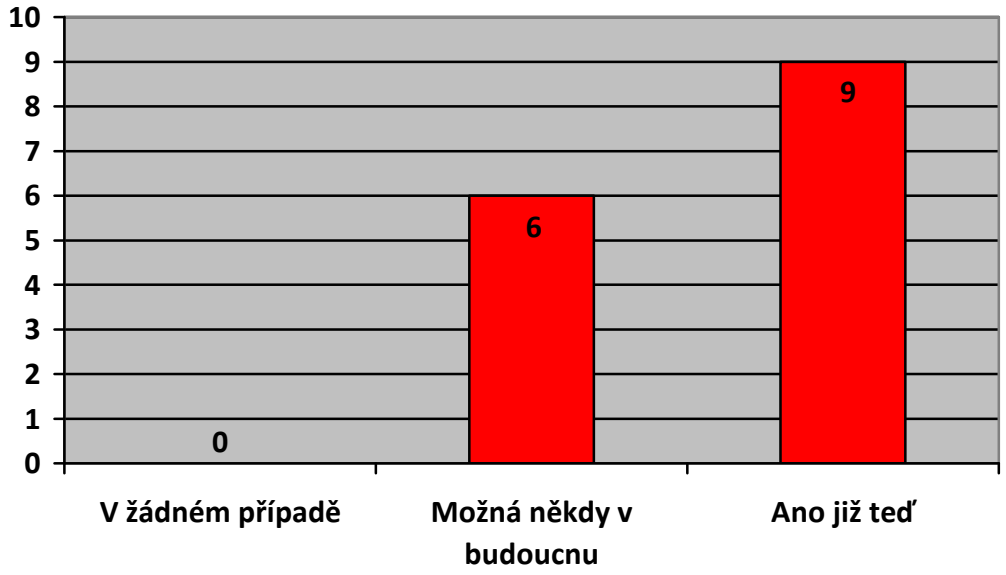


Graf 4 Poznal/a byste kyberteroristu podle vzhledu?

5.6 Existuje hrozba kyberterorismu v České republice?

V další, v pořadí páté, otázce respondenti vyjadřovali svůj názor nebo svou obavu, zda je pravděpodobnost určité hrozby kyberterorismu u nás, v České republice.

Všichni se shodli na tom, že určitá pravděpodobnost zde je, nikdo tedy nezvolil první možnost a to „v žádném případě“. Šest respondentů se domnívá, že v budoucnu zde taková hrozba být může a devět si myslí, že zde hrozba již je.

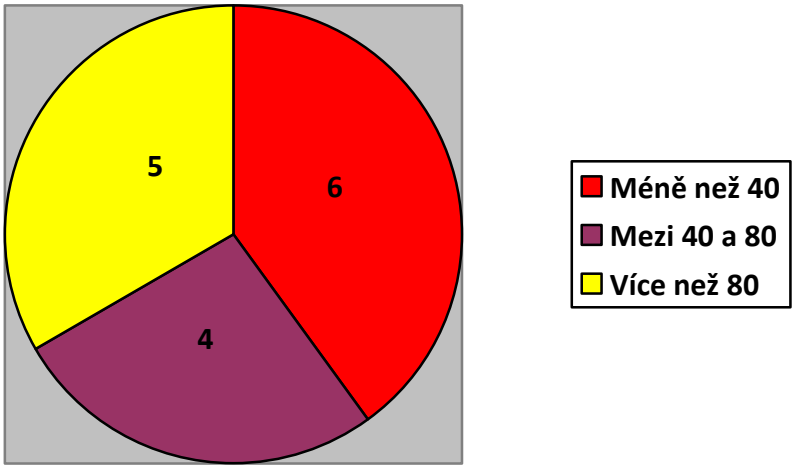


Graf 5 Existuje hrozba kyberterorismu v ČR?

5.7 Kolik už proběhlo kyberteroristických útoků ve světě?

Předposlední otázka se zaměřuje na počet již uskutečněných kyberteroristických útoků na celém světě. Nabídnuty byly tři možnosti, které zněly: „méně než 40“, „mezi 40 a 80“ a „více než 80“.

Zde jsou odpovědi opět vyrovnané. Šest a i nejvíc respondentů se domnívá, že jich bylo méně než 40, čtyři respondenti zvolili druhou možnost, a to, že doposud bylo mezi 40 až 80 kyberteroristickými útoky ve světě. Pět respondentů se rozhodlo pro poslední možnost, tedy nad 80 kyberteroristických útoků.

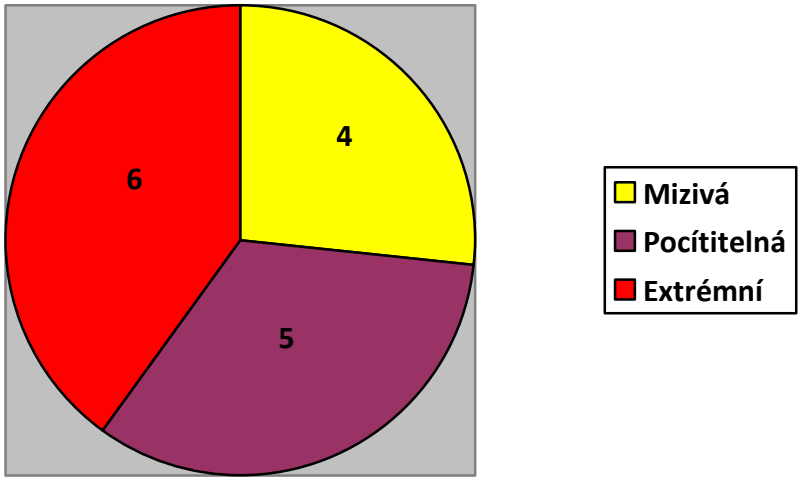


Graf 6 Kolik už proběhlo kyberteroristických útoků ve světě?

5.8 Jaká existuje šance zamezit dopadům kyberteroristických útoků?

Poslední otázka dotazníku. Respondentům byly nabídnuty tři odpovědi, „mizivá“, „pocítitelná“ a „extrémní“.

Čtyři si byli jistí odpovědí, že možnost zamezení dopadům je mizivá. Pět dalších si myslí, že kdyby byla snaha zamezit dopadům kyberteroristických útoků, tak by ji pocítili. A posledních šest respondentů odpovědělo, že šance je extrémní.



Graf 7 Jaká existuje šance zamezit dopadům kyberteroristických útoků?

5.9 Návrh na zvýšení informovanosti obyvatel

Zvýšení informovanosti obyvatel by vedlo ke zvýšení jejich obranyschopnosti. Je několik různých způsobů, jak toho docílit.

Lidé nadávají, že nejsou žádná preventivní sezení, oni by určitě přišli! Ve chvíli, kdy taková sezení uskutečníte, nepřijde nikdo, nebo jen pár jedinců. Ti vesměs přijdou, protože nemají nic lepšího na práci nebo je to opravdu zajímá. Tento způsob by byl sice také zajímavý, ale rozhodně by neměl dostatečné výsledky.

Zamyslíme-li se, každý jistě z hlavy dá dohromady minimálně 4 různá znění reklam. Nabízí se tu možnost vytvoření krátkých spotů, které by se pouštěli v televizích. Na všech programech. Spot by trval pár vteřin, musel by být zajímavý, chytlavý a nejlépe úsměvný, ale na druhou stranu nutící k zamyšlení. V takový okamžik se divákům do podvědomí dostane a donutí je nad daným problémem přemýšlet.

Jsou tu i tací, kteří televizi nemají, nebo ji provizorně nezapínají, je to přeci jenom žrout času. Dokud ještě fungují papírové formy novin, dají se do nich zakomponovat upozornění, texty, které nebudou dlouhé, zato výstižné. Takové, které stejně jako televizní spot donutí zamyslet se.

V konečné fázi, proč nevyužít stejné cesty, jako právě kyberteroristé. Využít kyberprostoru. Upozornění na nejfrekventovanějších stránkách, možnosti převedení na stránky zabývající se informovaností, apod.

Toto a mnohem více možností, letáčky v časopisech, novinách, billboardy, apod. je mnoho možností. Stačí se pouze zamyslet nad příklady, a další se dostavují samy.

Další možností, z úplně jiného oboru, jsou preventivní studentské přednášky. Dětem se na základních školách, případně na středních školách preventivně vypráví o kyberšikaně, jenž je mimo jiné taktéž součástí. Proč nezakomponovat i informování o takovém jevu?

Prodej přívěsků. Dělají se sbírky za různými účely, proč ne i za tímto. A z vytěžených peněz by se mohla financovat jiná osvěta, nebo zlepšit ochrana státu.

V komplexu těchto možností, jde možná až o přehnané typy, na druhou stranu, představíme-li si pouze jeden z nich, již reálnost a logičnost stoupá.

Je na každém z nás, jak se k problému kyberterorismu postavíme. Ale jedinec válku nikdy nevyhrál. Vždy měl někoho u sebe. Už pouze zvednutí informovanosti obyvatel zapříčiní větší obezřetnost a jako řetězec se spustí i větší bezpečnost.

6. ZÁVĚR

Riziko kyberterorismu zde je již od počátku kyberprostoru. Čím propracovanější kyberprostor je, tím je propracovanější jsou i útoky. A čím déle je přístupný, tím více času na přípravu útočníci mají. S pokroky, jenž jsou nabízeny vývojem technologie, vzrůstají i rizika. Přímá úměra v tomto směru funguje bezproblémově. Den ode dne se riziko útoku zvyšuje.

Kybernetická kriminalita nezná hranic, útoky bývají promyšlenější, závažnější a hůře zjistitelné. Nebo naopak obrovského rozsahu a téměř nezastavitelné. Právní systémy mají mezery, se kterými lze potrestat aktéry minimálně. V tomto ohledu je nutná změna. Dostaví-li se změny v právním systému, nezastaví to sice útoky jako takové, ale může to dopomoci demonstraci následků těchto činů. V České republice v trestním zákoníku nenalezneme jedinou skutkovou podstatu trestného činu vystihující kyberterorismus a trestající ho.

Cíle kyberteroristických útoků jsou velmi proměnné, nicméně prioritní zůstává kritická infrastruktura. S vývojem technologií se vyvíjí i cíle kyberterorismu.

Roste množství aktérů kyberteroristických útoků a jejich dovedností. Zlomové období pro kyberterorismus bylo 11. září 2001. Po tomto dni se množství kyberteroristických aktivit zvýšilo.

Analýza prokázala poměrně dobrou znalost okruhu kyberterorismu, ale stále jde pouze o obecné informace. Lidé vědí, že tu riziko je, nicméně si neuvědomují jaké. Nevidí rozdíl mezi kyberterorismem a kybernetickou kriminalitou. Tento rozdíl je málo patrný i studovaným lidem v oboru. Zlepšila-li by se situace skutkové podstaty trestnosti kyberterorismu, hranice by byly znatelnější.

Obecně je kyberterorismus velmi zajímavé téma, nutící k hledání dalších informací a novinek, neméně tak k zamyšlení. V této chvíli hrozba kyberterorismu pro Českou republiku není tak vysoká, jako například pro USA, Irán a podobné, ve světě známější státy. Do budoucnosti je ovšem více než vysoká, právě z důvodu zvýšené potřeby kyberprostoru pro „obyčejný“ život. Nezbývá tedy než stále posilovat bezpečnost státu a nepodceňovat soupeřovu sílu.

SEZNAM POUŽITÝCH ZDROJŮ

Seznam použitých českých zdrojů

JIROVSKÝ, V. *Kybernetická kriminalita*. 1. vyd. Praha: Granada, 2007 ISBN 978-80-247-1561-2

KOLEKTIV AUTORŮ POD VEDENÍM MZVČR. *Bezpečnostní strategie 2011*. Praha, 2011. ISBN 978-80-7441-005-5

Seznam použitých internetových zdrojů

MANA, Martin. Využívání informačních a komunikačních technologií v domácnostech a mezi jednotlivci 2012. In:*Český statistický úřad* [online]. 2012 [cit. 2013-01-14]. Dostupné z: http://www.czso.cz/csu/2012edicniplan.nsf/p/9701-12

Nové důkazy: Stuxnet fungoval minimálně od roku 2007. In: CONSTANTIN, L. a P. KREUZIGER. *Businessworld* [online]. QuinStreet Inc., 2013 [cit. 2013-03-04]. Dostupné z: http://businessworld.cz/novinky/nove-dukazy-stuxnet-fungoval-minimalne-od-roku-2007-10505

MVČR. ODBOR BEZPEČNOSTNÍ POLITIKY. *Definice pojmu terorismus* [online]. 2009 [cit. 2013-01-12]. Dostupné z: http://www.mvcr.cz/clanek/definice-pojmu-terorismus.aspx

SHANDRA. *Cyber Terrorism* [online]. [cit. 2013-01-05]. Dostupné z: http://cyberterrorismlaw.blogspot.cz/2012/03/history.html

[1] Černý Michal. *Kyberterorismus v informační společnosti. Část II*. Inflow: informatik journal [online] 2012 [citace 2013-03-04]. Dostupný z WWW: http://www.inflow.cz/kyberterorismus-v-informacni-spolecnosti-cast-ii. ISSN 1802-9736

[1] Černý Michal. *Kyberterorismus v informační společnosti. Část I.* Inflow: informatik journal [online] 2012 [citace 2013-03-04]. Dostupný z WWW: http://www.inflow.cz/kyberterorismus-v-informacni-spolecnosti-cast-ii. ISSN 1802-9736

SEZNAM OBRÁZKŮ, GRAFŮ a TABULEK

Seznam obrázků

Seznam grafů

SEZNAM PŘÍLOH

PŘÍLOHY

Příloha A – Dotazník

Dotazník – Kyberterorismus, co o něm víme?

Dobrý den,

ráda bych Vás požádala o malou laskavost. Vypracovávám bakalářskou práci na téma „Kyberterorismus, co o něm víme?“ A velice by mi pomohlo, kdybyste vyplnili tento krátký dotazník.

Dotazník je anonymní, pouze bych Vás požádala o vyplnění kategorie věku a pohlaví.

Věk: do 18 let 19-29 let 30-45 let 46-55 let více než 55 let

Pohlaví: žena muž

1. **Co si představíte pod pojmem kyberterorismus?**
   A. Terorismus s použitím zbraní hromadného ničení.
   B. Terorismus prostřednictvím počítačů, počítačových sítí a informací v nich
   C. Netuším

2. **Co si myslíte, že je důvodem kyberterorismu?**
   A. Nové technologie
   B. Krádeže osobních dat
   C. Obohacení se
   D. Anonymita
   E. Nepředvídatelnost síly a času útoku
   F. Jiné…….
   (Doplňte)

3. **Víte, kdy začalo období kyberterorismu?**

A. V 19. století
B. Ve 20. století
C. Ve 21. století

4. **Poznal/a byste kyberteroristu podle vzhledu?**
    A. Ano, určitě
    B. Ne
    C. Nevím

5. **Existuje hrozba kyberterorismu v České republice?**
    A. V žádném případě
    B. Možná někdy v budoucnu
    C. Ano, již teď

6. **Kolik už proběhlo kyberteroristických útoků ve světě?**
    A. Méně než 40
    B. Mezi 40 a 80
    C. Více než 80

7. **Jaká existuje šance zamezit dopadům kyberteroristických útoků?**
    A. Mizivá
    B. Pocítitelná
    C. Extrémní

Mockrát Vám děkuji za Váš čas a ochotu.

Najšlová Pavla, DiS.

BIBLIOGRAFICKÉ ÚDAJE

Jméno autora: Pavla Najšlová

Obor: Bezpečnostní studia

Forma studia: Kombinovaná

Název práce: Kyberterorismus, co o něm víme?

Rok: 2013

Počet stran textu bez příloh: 40

Celkový počet stran příloh: 2

Počet titulů českých použitých zdrojů: 2

Počet titulů zahraničních použitých zdrojů: 0

Počet internetových zdrojů: 6

Počet ostatních zdrojů: 0

Vedoucí práce: Ing. Michaela Havlová