ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta biomedicínského inženýrství
Katedra zdravotnických oborů a ochrany obyvatelstva

Kybernetické hrozby relevantní pro kritickou infrastrukturu České republiky

Relevant cyber threats to critical infrastructure, Czech Republic

Bakalářská práce

Studijní program: Ochrana obyvatelstva

Studijní obor: Plánování a řízení krizových situací

Vedoucí práce: Ing. Miroslav Nečas, Ph.D.

Jan Dovrtěl

Kladno, květen 2015

České vysoké učení technické v Praze, Fakulta biomedicínského inženýrství

Katedra zdravotnických oborů a ochrany obyvatelstva | Akademický rok: 2014/2015

Zadání bakalářské práce

Student:	**Jan Dovrtěl**
Obor:	Plánování a řízení krizových situací
Téma:	**Kybernetické hrozby relevantní pro kritickou infrastrukturu České republiky**
Téma anglicky:	Relevant cyber threats to critical infrastructure, Czech Republic

Zásady pro vypracování:

Cílem bakalářské práce bude zhodnocení vybraných kybernetických hrozeb a jejich možných dopadů na kritickou infrastrukturu České republiky. Zpracování teoretické části bude vycházet z platného zákona o Kybernetické bezpečnosti a dalších zdrojů týkajících se vybraného tématu. V praktické části bude provedeno zkoumání veřejných informací o útocích a hrozbách a analýza vybraných typů hrozeb a srovnání jejich vývoje v čase.
Bakalářská práce bude zpracována na základě metod obsahové a kontextové analýzy hlášení o hrozbách a analýzy časových řad. V přílohách budou uvedeny relevantní dokumenty týkající se tématu.

Seznam odborné literatury:

[1] GROS, I. , Kvantitativní metody v managerském rozhodování, ed. 1. vydání, 2003, ISBN 80-247-0421-8
[2] ŠENOVSKÝ M., ADAMEC V., ŠENOVSKÝ P., , Ochrana kritické infrastruktury, ed. 1. vydání, Ostrava: Edice SPBI Spektrum, 2007, ISBN 978-80-7385-025-8
[3] KÁCHA, P. , Adapting the ticket request system to the needs of CSIRT teams, 2009, WSEAS Transactions on Computers, 1109-2750

zadání platné do:	11.09.2016
Vedoucí:	Ing. Miroslav Nečas, Ph.D.
Konzultant:	doc. Ing. Václav Čuba, Ph.D.

l. s.

vedoucí katedry / pracoviště | děkan

V Kladně dne 23.02.2015

Prohlášení

Prohlašuji, že jsem bakalářskou práci s názvem *Kybernetické hrozby relevantní pro kritickou infrastrukturu České republiky* vypracoval samostatně a to za použití citací použitých pramenů, které uvádím v seznamu přiloženém k bakalářské práci.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 Zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Praze dne 20. března 2015 . . . . . .

Podpis

Poděkování

Na tomto místě bych rád poděkoval vedoucímu práce panu Ing. Miroslavovi Nečasovi, Ph.D. za věcné připomínky, podnětné návrhy a pomoc při realizaci mé bakalářské práce.

Abstrakt

Bakalářská práce „Kybernetické hrozby relevantní pro kritickou infrastrukturu České republiky“ se zabývá Národním kybernetickým centrem, které vzniklo na základě přijetí usnesení vlády České republiky ze dne 19. října 2011. V praktické části se práce zabývá hackerskými útoky v rámci operace AntiSec, ze kterých si lze vzít příklad jako z možných útoků na kritickou infrastrukturu nebo významné informační systémy České republiky. Závěrem je provedeno celkové zhodnocení vybraných kybernetických hrozeb a jejich možných dopadů na kritickou infrastrukturu nebo na významné informační systémy České republiky.

Klíčová slova

Kybernetické hrozby, kritická infrastruktura, AntiSec, Anonymous, LulzSec

Abstract

The Bachelors Thesis „Relevant cyber threats to the critical infrastructure, Czech Republic" describes the role of The National Cyber Security Centre (NCSC) that was established according to the Decision n. 781 of the Government of the Czech Republic from 19th October 2011. In the practical part of the Thesis cyber-attacks within the cybernetic campaign "Operation AntiSec" (#opAntiSec) are used as an example of possible threats to the Critical Infrastructure of the Czech Republic and to the Information Systems of the Government. Based on the analysis of these attacks are defined possible impacts of similar threats to the Critical Infrastructure of the Czech Republic and Government Information Systems are evaluated.

Key words

Cybernetic Threats, Critical Infrastructure, AntiSec, Anonymous, LulzSec

Obsah

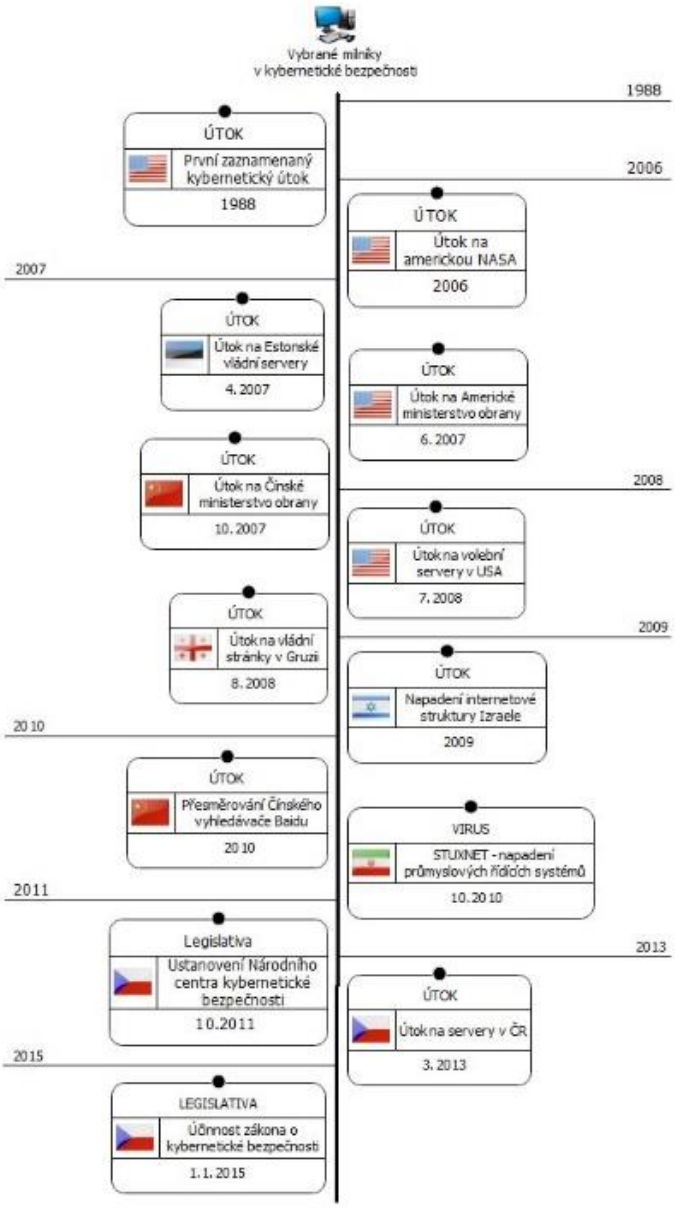
1 Úvod

Téma své bakalářské práce „Kybernetické hrozby relevantní pro kritickou infrastrukturu České republiky“ jsem si zvolil z důvodu, že již 15 let pracuji jako referent státní správy Národního bezpečnostního úřadu, který se stal dne 19. října 2011 usnesením vlády České republiky č. 781 gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast. Osobně nejsem po pracovní stránce součástí tohoto programu, nicméně tato oblast mne zajímá a myslím si, že každý kdo ve svém životě používá informační technologie, je v podstatě jedno v jaké podobě, by měl mít alespoň dílčí povědomí o rizicích, která jsou s tím spojena. V této bakalářské práci bych chtěl sobě i čtenáři rozšířit povědomí o rizicích a hrozbách, které měly a v budoucnu i mohou mít dopad na stále se rozšiřující závislost lidstva na kybernetickém prostoru a informačních technologiích obecně. Rád bych také ověřil hypotézu, zda existuje vztah mezi impulzem a samotnou realizací kybernetického útoku. Pokud by se tato hypotéza potvrdila, mohlo by být nalezeno řešení jak útokům předcházet nebo se jim zcela vyvarovat.

2 Nejzávažnější kybernetické útoky v minulosti

S nástupem informačních technologií a používáním výpočetní techniky obecně vzniklo i riziko jejich zneužití. Nárůstem a rozmachem tohoto odvětví a začleněním do každodenního života člověka se rizika neustále zvyšují.

Graf č. 1 – Vybrané milníky vynesené do časové osy



Zdroj: vlastní zpracování autora

První zaznamenaný kybernetický útok na rodící se počítačovou infrastrukturu se datuje do roku 1988. V tomto roce byl vypuštěn tzv. červ zvaný Morris, který využíval

nedostatky v systému UNIX Noun 1. Šířil se z velké části v USA a zpomaloval počítače až do jejich nepoužitelnosti. Tento červ byl dílem Roberta Tappana Morrise, který na svou obhajobu říkal, že se snažil odhadnout velikost tehdejšího internetu. Následně byl jako první odsouzen za počítačové podvody. (NATO, 2015)

Následoval další útok a to konkrétně v prosinci 2006 na americkou NASA, která byla nucena blokovat e-mailové zprávy s přílohami, neboť bylo podezření, že se neznámí útočníci snaží získat informace o probíhajícím programu kosmických nosných prostředků. (NATO, 2015)

Kybernetický útok v dubnu roku 2007 byl směrován na estonské vládní servery a banky. Atakovány byly: stránky prezidentského úřadu a parlamentu, téměř všechny vládní ministerstva země, politické strany, tři ze šesti největších zpravodajských organizací, dvě největší banky a firmy specializující se na komunikace. Estonci reagovali velice pružně, především zamezením zahraničnímu přístupu za účelem zachování provozu pro domácí uživatele. (BÍLÝ, 2012)

Následovaly útoky:

Červen 2007 – Útok na Ministerstvo obrany spojených států amerických na e-mailové účty a síť Pentagonu. Firewall nedovedl útoky zachytit pro jejich sofistikovanost. Pentagon byl nucen na tři týdny odpojit celou síť. Tehdejší odborníci spekulovali, že za útoky je čínská vláda.

Říjen 2007 – Útok na Čínské ministerstvo bezpečnosti, byly odcizeny informace o čínských klíčových oblastech. Zveřejněné informace uváděly, že útok byl veden z Tchaj-wanu (42%) a ze Spojených států amerických (25%).

Léto 2008 – Napadení databáze republikánských i demokratických kampaní vedených k prezidentské volbě v USA. Za útočníky byly označeny jednotky Čínské lidové republiky. Útoky měly demonstrovat slabou národní bezpečnost USA. Napadány byly hlavně počítače a notebooky asistentů a poradců obou prezidentských kandidátů. Tyto útoky spadaly do kategorie kybernetická špionáž.

Srpen 2008 – Napadení počítačové sítě v Gruzii. Vládní stránky byly nahrazeny jinými stránkami. Sám o sobě neměl tento útok žádný dopad, ale spekulovalo se o tom, že útočníci kooperovali s ruskými vojenskými akcemi.

Leden 2009 – Napadena internetová infrastruktura Izraele. V průběhu vojenské ofenzivy v pásmu Gazy v lednu 2009 byly vedeny útoky na stránky izraelské vlády z cca 5 mil. počítačů. Spekulovalo se o tom, že byl útok veden z některého státu bývalého Sovětského svazu. Financován měl být hnutím Hamás nebo Hizballáh.

Leden 2010 – Skupina s názvem "Iranian Cyber Army" narušila službu populárního čínského vyhledávače Baidu. Uživatelé byli přesměrováni na stránku zobrazující íránské politické poselství. Stejná "Iranian Cyber Army" se nabourala do Twitteru o měsíc dříve s podobnou zprávou.

Říjen 2010 – Objeven Stuxnet, malware vyvinutý pravděpodobně již v roce 2007, byl navržen tak, aby napadal průmyslové řídicí systémy Siemens (WinCC, Step7), ze kterých jsou sledovány specifické automaty (S7-300) s připojenými moduly (CP-342-5) pro řízení frekvenčních měničů. Červ se aktivoval pouze v případě, že konfigurace a počet centrifug na obohacování uranu odpovídal Íránskému závodu v Natanzu. Následně upravil software PLC, tak aby docházelo k opakované změně výstupní frekvence měničů. Aby zamaskoval svoji činnost, podstrčil do Step7 své DLL knihovny tak, aby uživatel infikovaného počítače měl pocit, že v PLC se nachází původní nepoškozený software. Součástí Stuxnetu byla i funkce pro připojení ke vzdálenému internetovému serveru, aby od něj červ přijal další příkazy a mohl jej informovat o své činnosti. Útoku na Írán odpovídá i to, že ze 45 000 (jak uvedl Microsoft v srpnu 2010) napadených počítačů leželo 60 % v Íránu, 18 % v Indonésii a 8 % v Indii (podle firmy Symantec). Celková sofistikovanost viru vede experty k domněnce, že se jedná o profesionální práci s největší pravděpodobností armádního původu, např. Izraele, prostřednictvím Jednotky 8200 (NATO, 2015)

Tímto velmi zkráceným výčtem významnějších kybernetických útoku, uvedených na webových stránkách Severoatlantické aliance (dále jen „NATO“), jsem chtěl nastínit, o jak závažnou problematiku se jedná a s jakou progresí či sofistikovaností jsou kybernetické útoky vedeny. Rovněž jsem chtěl i upozornit na fakt, že kybernetická

bezpečnost není jen chimérou a přijetí zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „zákon o kybernetické bezpečnosti“) bylo nutností.

Konkrétními útoky na Českou republiku (dále jen „ČR“) byly 4. března roku 2013 poškozeny zpravodajské servery ihned.cz, idnes.cz, novinky.cz, lidovky.cz, denik.cz, E15.cz, zive.cz a mobilmania.cz. Následovaly útoky na servery finančních institucí csob.cz (ČSOB), rb.cz (Raiffeisen Bank), kb.cz (Komerční banka), csas.cz (Česká spořitelna), fio.cz (Fio Banka) a pse.cz (Prague Stock Exchange BCPP). 7. března 2013 si útočníci vybrali za cíle servery společností T-mobile, O_2, Dopravního podniku Hl. m. Prahy, České televize a zpravodajského portálu ČT24. Tyto zmiňované útoky byly typu DDoS, které znepřístupnily tyto servery potencionálním návštěvníkům. Nejednalo se tudíž o příliš závažný útok, ale dokazuje nám, že ČR není výjimkou a kybernetické hrozby jsou reálné i na našem území.

3 Kybernetická bezpečnost

Kybernetická bezpečnost je pojem všeobecně rozšířený na počátku současného tisíciletí. Jedná se o pojem související s rozvojem informačních technologií a „internetovým“ vnímání společnosti. Jedná se o pravidla, povinnosti a zásady, které by měly být závazné pro každého provozovatele či uživatele informačních technologií.

3.1 Bezpečnostní hrozby, události, incidenty

Na základě analýzy aktiv a jejich zranitelných míst bylo nutno identifikovat možné bezpečnostní hrozby, které mohou napadnout konkrétní zranitelné místo konkrétního aktiva. Tedy popsat možnou hrozbu včetně možného zdroje hrozby, případně úmyslnost a motivaci útočníka, vliv hrozby na jednotlivé atributy informační bezpečnosti aktiva (dostupnost, integritu, důvěrnost). Součástí analýzy hrozby byl i odhad pravděpodobnosti, případě možné frekvence hrozby.

Vývoj informačních a komunikačních technologií (dále jen „ICT“) s sebou přináší nové a nové bezpečnostní hrozby, které se neustále vyvíjí. Analýza hrozeb se tedy u každého aktiva a každého informačního systému musí dělat opakovaně.

Situaci, kdy se hrozba pokusí působit na zranitelné místo s cílem ohrozit informační bezpečnost aktiva, se říká bezpečnostní událost. Pokud se působením hrozby naruší vlastnosti aktiva natolik, že dojde k narušení informační bezpečnosti, vzniká bezpečnostní incident. Bezpečnostní incident je tedy stav aktiva a bezpečnostní událost aktivita, která k tomuto stavu vede. Pro pochopení tohoto rozdílu můžeme uvést příklad: neoprávněné otevření dveří do datového centra považujeme za bezpečnostní incident a činnosti, které k němu mohou vést (například útok hrubou silou, manipulace se zámkem, neoprávněné použití klíčů, uvedení oprávněné osoby v omyl, atd.) budeme chápat jako bezpečnostní události. (PŘECH, 2014)

3.1.1 Rozdělení hrozeb

Níže popsané rozdělení hrozeb uvádí server kybez.cz jako jednu z možných variant, které lze vzít v úvahu. Jejich rozdělování je subjektivní.

PODLE ZDROJE PŮSOBENÍ:

- hrozby vnitřní vycházející ze samotného aktiva (např. výrobní vada)

- hrozby vnější, jejichž zdroj je mimo vlastní aktivum

PODLE ÚMYSLU:

- náhodné hrozby (přírodní katastrofa, výpadek proudu)
- neúmyslné hrozby (omylem vymazaný soubor)
- úmyslné hrozby (úmyslné poškození, zcizení, síťový útok)

PODLE PŮVODU (SUBJEKTU INICIACE):

- přírodní hrozby (blesk, zemětřesení)
- hrozby způsobené člověkem (odposlech, chyba uživatele)

PODLE TOHO, NA JAKÝ DRUH AKTIVA PŮSOBÍ:

- hrozby pro hardware
- hrozby pro síť
- hrozby pro operační systém
- hrozby pro aplikace
- hrozby pro informace
- hrozby pro uživatele

PODLE SMĚROVÁNÍ NA BEZPEČNOSTNÍ ATRIBUTY:

- hrozby dostupnosti (DDOS útok, požár)
- hrozby integrity (chyba v databázové transakci)
- hrozby důvěrnosti (krádež notebooku)

PODLE MOTIVACE ÚTOČNÍKA:

- hrozby za účelem získání finančního prospěchu
- hrozby za účelem získání konkurenční převahy
- hrozby za účelem dokázání svých schopnost
- hrozby za účelem odplaty
- hrozby z důvodu neplnění povinností

3.1.2 Relevantní hrozby

Server hackmageddon.com rozděluje hrozby na hacktivismus, kybernetickou kriminalitu, kybernetickou špionáž a kybernetickou válku. Pod tyto termíny lze zahrnout veškeré aktivity, které budou popisovány v další části. Hactivismus je akt hackování (rozlamování), nebo vloupání se do počítačového systému, tento akt je sociálně nebo politicky motivovaný. Počítačová neboli kybernetická kriminalita (cybercrime, kyberzločin) je trestná činnost, ve které jistým způsobem figuruje počítač

obecně. Případně některá jeho část nebo komponenta, či větší množství počítačů samostatných, nebo propojených v počítačových sítích. (JIROVSKÝ, 2007) Kybernetickou špionáž lze definovat jako prozrazení výrobního postupu či neoprávněné kopírování dat za pomoci počítače. (PŘIBYL, 2014) Kybernetickou válku můžeme popsat jako válku, při které jsou vedeny útoky na datová centra, servery, států nebo jednotlivých stran, kde jsou cílem data, peníze, informace, vypnutí internetových služeb apod. Vojáci jsou lidé a zbraně jsou mobilní telefony servery nebo počítače (ŠNAJDR, 2015).

4 Přiměřenost přijatých opatření proti kybernetickým hrozbám

Absolutní bezpečnost nelze v rámci přijímání zákona o kybernetické bezpečnosti dosáhnout. Česká republika přijme reálná opatření, která se budou zakládat na hodnocení a analýze rizik a budou s těmito riziky korespondovat. Přijatá opatření budou v první řadě zohledňovat základní práva a ochranu soukromí. Tím je myšlena svoboda projevu, svobodný přístup k informacím apod. Přijatá opatření budou přiměřená k hrozícímu nebezpečí a zároveň budou respektovat základní práva. (NCKB, 2012)

4.1 Cíle, opatření - strategie

Akční plán definuje přesné úkoly a zároveň určuje subjekty kompetentní k jejich řešení. Tento Akční plán vychází ze strategie zaměřené na současné a aktuální hrozby a opatření proti nim. Prvotně byla řešena tvorba legislativního rámce ve strategické oblasti.

Národní bezpečnostní úřad (dále jen „NBÚ“) vytvořil ve své oblasti unikátní zákon, kterým jsou vymezeny činnosti a odpovědnost Národního centra kybernetické bezpečnosti (dále jen „NCKB“). Zákonem jsou definovány závazné úkoly dané subjektům, které tvoří nebo užívají informační nebo komunikační technologie v kybernetickém prostoru. Určuje také formu, způsob a rozsah kooperace s veřejným sektorem, soukromým sektorem a mezinárodními subjekty.

Strategie sleduje, analyzuje a následně vyhodnocuje trendy, smlouvy a doporučení v mezinárodní legislativě, které se dotýkají kybernetické bezpečnosti a informačních technologií obecně. Získané poznatky byly následně zavedeny a i nadále budou zaváděny do praxe tak, aby byla ČR plnohodnotným spolupracovníkem na poli kybernetické bezpečnosti se státy Evropské unie a NATO, případně dalších spolupracujících organizací. (NCKB, 2012)

4.2 Vytvoření Národního centra kybernetické bezpečnosti a vládního CERT pracoviště

Aby došlo ke zlepšení koordinace a spolupráce mezi jednotlivými subjekty nejen v rámci státní správy v oblasti ochrany a zavedení protiopatření při kybernetických

incidentech bylo při NBÚ zřízeno NCKB jehož součástí je vládní Computer Emergency Response Team (dále jen „CERT“).

NCKB je koncipováno tak, aby těsně spolupracovalo s dalšími orgány státu, soukromými subjekty a akademickými pracovišti. Tato spolupráce je smluvně podložena, aby NCKB mohlo rychle a efektivně sdílet informace o odhalených slabých místech, zranitelnosti ICT, formách útoků, motivaci a profilech útočníků. Tím by také měla být zajištěna možnost, neprodleně a operativně analyzovat jednotlivé incidenty, na něž by následně vydávalo doporučení k potřebným opatřením. Soukromý sektor při ochraně svých informačních i komunikačních systémů má zájem o spolupráci s NCKB, neboť jej vnímá jako prostředek včasného varování a umožňuje mu prevenci a přípravu na možný útok. S tím souvisí i příprava systému včasného varování před kybernetickými útoky.

Stejně jako složky Integrovaného záchranného systému testují zavedené procesy, bude i NCKB prosazovat přezkum účinnosti opatření a zvládání bezpečnostních incidentů jako součást řízení rizik. Tyto schopnosti se budou testovat na všech úrovních. Výstupy z těchto cvičení se analyzují a poznatky se budou zavádět do praxe.

4.3 Kybernetická bezpečnost informačních a komunikačních systémů veřejné správy - posilování

Pro bezpečné využívání kybernetického prostoru je nutné zajistit včasné, relevantní a ucelené informace o zjištěných rizicích. Na stránkách govcert.cz bude takové informace NCKB zveřejňovat. Na stejném webu budou také publikovány dostupné produkty a služby využitelné v dané oblasti.

Jedním z nezbytných předpokladů pro posílení bezpečnosti informačních systémů je zavedení závazných standardů a norem. Aby byla kybernetická bezpečnost efektivní, musí orgány veřejné správy povinně implementovat a důsledně dodržovat tyto normy a standardy s pravidelnou a důslednou kontrolou.

NKCB počítá s postupným zaváděním ISMS (Information Security Management Systém) ve veřejné správě, což by mělo zajistit zlepšení bezpečnostní úrovně informačních systémů a to formou metodických materiálů doporučených postupů a směrnicemi. Spolupracováním s orgány činnými v trestním řízení bude NCKB využívat

poznatky a následně je zavádět do praxe, tak aby přispělo k potírání kybernetické kriminality.

4.4 Evropská kybernetická bezpečnost – spolupráce s NBÚ

Aby bylo dosaženo bezpečnosti v kybernetickém prostoru, je nutné koordinovat spolupráci nejen v národním, ale i mezinárodním měřítku.

Ve spolupráci s Evropskou unií bude NBÚ rozvíjet opatření totožná s evropským Akčním plánem zaměřeným na ochranu kritických informačních infrastruktur. Další spolupráce bude probíhat v oblasti školení, výcviku a cvičení s Evropskou agenturou pro bezpečnost informací a sítí. Inspirací pro následné aktivity mohou být i organizace „Strategie vnitřní bezpečnosti EU", "Digitální agenda pro Evropu" a "Politika NATO v oblasti kybernetické obrany“. NBÚ bude prostředníkem ve spolupráci s Evropskou agenturou pro řízení velkých informačních systémů v oblasti bezpečnosti a práva a Evropským centrem počítačové kriminality.

4.5 Důvěryhodné informační technologie a jejich používání

Aby měli uživatelé informačních a komunikačních prostředků veřejné správy možnost využívat spolehlivé systémy, bude nutné podporovat výzkum a vývoj prostředků na jejich ochranu. Důvěryhodnost programových prostředků a technických prostředků v kritických oblastech důležitých pro státní bezpečnost, by měla být zajištěna v prvé řadě využíváním hodnocených a normalizovaných prostředků podle mezinárodních standardů.

4.6 Osvěta v oblasti kybernetické bezpečnosti

Nedílnou součástí při vytváření standardu kybernetické bezpečnosti je osvětová činnost cílená na správce a administrátory informačních systémů, vývojové pracovníky, auditory, vedoucí pracovníky a hlavně na samotné koncové uživatele. Neinformovanost v této oblasti představuje velké riziko stejně jako nedostatek personálu s aktuálním povědomím o zabezpečení ICT. Koncoví uživatelé budou relevantní informace získávat prostřednictvím sdělovacích prostředků. Kybernetická bezpečnost bude školena ve veřejné správě prostřednictvím vzdělávacích kurzů se snahou toto rozšířit a prosadit i do soukromé sféry. Cíl takovéto osvěty je v úrovni znalostí jednotlivých zaměstnanců a

jejich rolích v kybernetické bezpečnosti. Osvětová činnost bude neustále analyzována a upravována tak, aby odrážela aktuální potřeby.

4.7 Odezva na kybernetické útoky

Kybernetické útoky se v dnešní době stávají součástí našeho života. Aby bylo možné systémy veřejné správy a subjekty kritické infrastruktury chránit, musíme na ně být připraveni. Spoluprací s kompetentními institucemi byl vytvořen ucelený a koordinovaný soubor opatření, která budou při kybernetickém útoku aplikována. Při vytváření tohoto souboru opatření se přihlíželo k jejich nezbytnosti a přiměřenosti.

NCKB ve svém dokumentu „Strategie a Akční plán“ říká: „*Strategie pro oblast kybernetické bezpečnosti České republiky na období 2012-2015 navazuje na Bezpečnostní strategii České republiky a reflektuje výzvy moderní informační společnosti. Strategie je institucionálním rámcem, který dotváří bezpečnostní systém České republiky. Tento rámec je počátkem aktivní politiky kybernetické ochrany státu, kterou je nutné neustále vyhodnocovat a dotvářet. Povědomí každého jednotlivce, provozovatele, správce, univerzity nebo firmy o bezpečnostních výzvách ICT, je základním předpokladem k zajištění spolehlivosti a bezpečnosti kybernetického prostoru. Česká republika vnímá problematiku kybernetické bezpečnosti jako důležitou součást každodenního využívání ICT a bude nadále realizovat opatření k jejímu zajištění.“* (NCKB, 2012)

5 Záměr zákona o kybernetické bezpečnosti

Abychom byli schopni čelit kybernetickým útokům, bylo třeba zmapovat stávající stav, stanovit co nás ohrožuje, kde jsme zranitelní, a kdo by měl případný prospěch z provedených útoků. Na základě analýzy rizik pak stanovit případnou obranu nebo ochranu.

5.1 Vnější vlivy

Závislost lidstva a jeho fungování na technologiích narůstá geometrickou řadou ve všech směrech. S nárůstem závislosti společnosti na technologiích současně vzrůstá i riziko zneužití těchto technologií, které může mít rozsáhlé dopady. To se netýká pouze subjektů, které je provozují ale i jejich uživatelů, případně to může vést i k finančním či osobním škodám.

Obecně je celosvětová snaha zajistit přiměřenou ochranu těchto technologií před napadením, které by mohlo ohrozit nebo narušit jejich chod. Útoky vedené na informační technologie jsou globálním problémem, který nezná hranic. Dopady způsobují nejen ekonomické škody, nevyhýbají se státnímu ani soukromému sektoru a jsou schopny vyvolávat důsledky na vnitrostátní i na nadnárodní úrovni. Pokud dojde na útok, který je veden na některý z prvků kritické infrastruktury, může být ohrožena bezpečnost případně i samotná existence státu.

Sofistikovanost útoků na informační systémy se stále zdokonaluje. Pokud byli dříve útočníci motivováni pouze ekonomickou stránkou, s postupem doby se problematika rozšířila o kybernetický terorismus a o kybernetickou špionáž. Jedním z možných cílů by v budoucnu mohl být i některý z prvků kritické infrastruktury. Jako prvky kritické infrastruktury si můžeme představit systémy elektráren, systémy veřejné správy nebo informační systémy zdravotnictví.

Pokud přihlédneme k faktu, že kyberprostor nezohledňuje geografické hranice, je třeba útoky na informační technologie řešit na nadnárodní úrovni. Vzhledem k faktu, že ČR je členem NATO a Evropské unie (dále jen „EU“), byl na ni vyvíjen tlak na řešení celé problematiky formou závazné právní regulace.

Kybernetická bezpečnost je a bude jednou ze stránek celkové bezpečnosti České republiky. Veškeré vyspělé státy, kam se bezesporu i ČR řadí, jsou zcela závislé na funkčních ICT. Funkční informační systémy jsou jednou z podmínek pro rozvoj konkurenceschopnosti dané společnosti. „Informační společnost“ je společnost využívající technologie a zařízení. S tím související činnosti jsou v současné době velmi dynamicky se rozvíjejícím sektorem všech moderních ekonomik, na kterém je stavěna ekonomická prosperita a možná i životní úroveň občanů. Zabezpečení kyberprostoru je jedním z kritérií, ke kterým přihlíží zahraniční investoři, může do jisté míry ovlivnit konkurenceschopnost regionu.

Pokud přihlédneme k faktu, že ekonomická aktivita se stále více přiklání k informačním technologiím, tím se zvyšuje i hrubý domácí produkt a je nezbytné zajistit i bezproblémovou funkčnost tohoto prostředí, tudíž je nutné investovat do kybernetické bezpečnosti.

S rozmachem sociálních sítí, vnitropodnikových sítí, sítí hráčů apod. se z internetového prostoru stal prostředek, kterým lze společnost v širokém slova smyslu stimulovat a to jak negativně tak i pozitivně. (MALÝ, 2012)

5.2 Vnitřní vlivy

Ochrana kybernetické prostoru a bezpečnost v ČR byla řešena soukromoprávními subjekty bez jakékoliv regulace. Speciální pracoviště řešilo případné útoky na technologie bez centrální úrovně. Nemělo přístup k řešení již uskutečněných útoků a bylo tudíž nuceno případy řešit individuálně, což zvyšovalo nejen náklady ale i čas.

Veřejná správa nedisponovala jednotným způsobem jak postupovat v případě bezpečnostních incidentů, narušení jejích informačních systémů, kterými by minimalizovalo škody. Stejně tak nebyla řešena prevence či včasné varování, které by systémově minimalizovalo tyto útoky. Jak pronikala elektronizace do soukromého sektoru, probíhala i ve veřejném sektoru. Kybernetické hrozby byly a jsou stále aktuálnější, bylo tedy nezbytností zajistit opatření, které by státu a státní správě umožnilo centralizovaně reagovat na tyto hrozby, stejně jak je tomu na základě zkušeností v ostatních státech.

Obecně je známo, že státní moc lze uplatnit pouze na základě zákona a povinnosti soukromoprávních subjektů lze uložit jen zákonem, bylo tedy třeba kybernetickou bezpečnost regulovat zákonem, s jasným rozdělením povinností. Subjekty důležité pro veřejnou správu a ostatní subjekty by měly vymezené role a sjednocené pojmy užívané v oblasti kybernetické bezpečnosti.

Pokud by nebyla přijata výše uvedená opatření, hrozil by nárůst kybernetických útoků, případné materiální škody a ohrožení kritické infrastruktury ČR, což by mělo za důsledek i neplnění závazků smluvně ukotvených v ochraně investic.

Dalším, ne však posledním, vnitřním vlivem bylo i přijetí usnesení vlády ČR č. 781 ze dne 19. října 2011 o ustavení NBÚ řešitelem problematiky v oblasti kybernetické bezpečnosti a národní autoritou. Usnesení, mimo jiné, uložilo NBÚ zbudovat funkční NCKB a to do konce roku 2015. (MALÝ, 2012)

5.3 Cílový stav v oblasti kybernetické bezpečnosti

Cílem kybernetického zákona bylo zřídit systém výkonného mechanismu na bázi spolupráce v oblasti kybernetické bezpečnosti mezi soukromým a veřejným sektorem, který zvyšuje efektivitu v řešení kybernetických hrozeb. Uvádí v praxi soubory povinností a oprávnění. Zákon nastavuje předvídatelné transparentní postupy pro subjekty, které jsou nebo mohou být zahrnuty do zákonné regulace, spočívající v dílčích krocích zajišťujících podrobnější přehled o hrozbách a rizicích vyskytujících se v kybernetickém prostoru. Tím bude zajištěna možnost rychlé reakce na nové hrozby, které mohou nastat. Záměr kybernetického zákona si nekladl za cíl eliminovat či postihnout veškerá rizika dotýkající se všech uživatelů, snažil se řešit infrastrukturu významnou pro fungování státu, která by v případě narušení měla za následek poškození, případně ohrožení zájmu ČR. Subjekty, kterých se zákon dotýká, mají stanoveny přesné povinnosti, jejímž prostřednictvím dojde k navýšení ochrany jejich informačních systémů a infrastruktury, kterou provozují. Zákonem uložené povinnosti jsou veskrze marginální, nicméně zajistí dosažení kýženého cíle. Ostatním uživatelům budou předkládána doporučení včetně závěrů z praxe. (MALÝ, 2012)

Cíle stanoveny v kategoriích, jak je uvádí „Návrh pro vnější připomínkové řízení“ NBÚ: „…

- *Konstituce práv a povinností orgánu státu, jemuž je svěřena konkrétní pravomoc v oblasti zajišťování kybernetické bezpečnosti v souvislosti s právy a povinnostmi dalších orgánů státu a soukromoprávních subjektů, které v této oblasti participují.*

- *Nastavení mechanismu přenosu informací nezbytných pro prevenci před kybernetickými hrozbami, které budou sloužit pro analýzu možných kybernetických útoků a pro způsoby jejich včasného rozpoznání.*

- *Vybudování systému včasného varování, prevence a osvěty včetně poskytování pomoci při zavádění preventivních opatření a protiopatření při hrozícím útoku.*

- *Standardizace nastavení bezpečnosti systémů nezbytných pro chod státu v rámci kritické informační infrastruktury státu.*

- *Stanovení pravidel pro koordinaci činností pro odvrácení a při odvracení hrozícího útoku na prvky kritické informační infrastruktury státu a k řešení situací, v nichž je potřeba přijímat opatření před možným následkem hrozícího útoku.*

Konečným cílem uvedených aktivit je vytvoření a udržení důvěryhodné a konkurenceschopné informační společnosti, s důrazem na rozvoj svobodného a bezpečného využívání a sdílení informací a v neposlední řadě i zlepšení obrazu státu v této oblasti, a to jak v kontextu národním i mezinárodním". (NBÚ, 2012)

6 Vyhláška k zákonu o kybernetické bezpečnosti

Vyhláška k zákonu o kybernetické bezpečnosti stanovuje obsah a strukturu bezpečnostní dokumentace, řešení bezpečnostních opatření a šíři jejich aplikování, typy a kategorie kybernetických incidentů, jakým způsobem hlásit kybernetický bezpečnostní incident, informovat o provedených opatřeních a o jejich výsledku. Vyhláška dále stanovuje vzor oznamování kontaktních údajů a jeho formu. Tím by mělo být dosaženo sjednocení a stanovení normy náhledu a komunikace při řešení jednotlivých incidentů.

6.1 Definice

Ustanovením § 28 odst. 1 zákona č. 181/2014 Sb., o kybernetické bezpečnosti byli zmocněni Ministerstvo vnitra a NBÚ vydáním vyhlášky o významných informačních systémech a jejich určujících kritériích. Toto ustanovení bylo publikováno ve Sbírce zákonů dne 29. srpna 2014 a účinnosti dnem 1. ledna 2015.

Zákon o kybernetické bezpečnosti se snaží uvést v praxi soubory povinností a pravomocí, které by zvýšily bezpečnost v kybernetickém prostoru. Snaží se nastavit systém výkonného mechanizmu na bázi spolupráce v oblasti kybernetické bezpečnosti mezi soukromým a veřejným sektorem, který by zvýšil efektivitu v řešení kybernetických hrozeb. Nepředpokládá však, že svým zavedením eliminuje veškerá rizika napříč všemi uživateli kybernetického prostoru. Snaží se chránit významné informační systémy a část kritické infrastruktury ČR, která je závislá na informačních technologiích. Subjekty, kterých se zákon dotýká, mají stanoveny přesné povinnosti, jehož prostřednictvím dojde k navýšení ochrany jejich informačních systémů, infrastruktury, kterou nebo které provozují. Povinnosti uložené zákonem jsou minimální, nicméně zajistí dosažení kýženého cíle.

Jde hlavně o zavedení povinnosti činit bezpečnostní opatření, dokumentovat a detekovat bezpečnostní incidenty, které je třeba následně nahlásit. Zavádět opatření, která vydá NBÚ. Informovat o případných změnách kontaktních údajů. Povinnosti uložené zákonem o kybernetické bezpečnosti jsou uloženy správcům významných informačních systémů a kritické informační infrastruktury. Kritická informační infrastruktura bude určována způsobem stanoveným v zákoně č. 240/2000 Sb., krizový

zákon. V prováděcím právním předpisu v souladu s § 28 zákona o kybernetické bezpečnosti budou následně určeny i významné informační systémy.

6.2 Právní stav v oblasti kybernetické bezpečnosti

V České republice je kybernetická bezpečnost upravována zákonem č. 181/2014 Sb. (Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů). Současně i ostatní platné právní úpravy řeší dílčí problematiku kybernetické bezpečnosti jako je odpovědnost za delikty, certifikaci zabezpečení komunikačních a informačních systémů, které nakládají s utajovanými informacemi. Zákon č. 181/2014 Sb. a prováděcí předpisy jsou prvním celkem v České republice, které řeší tuto oblast v rámci prevence i aktivně formou reakce na případný výskyt bezpečnostního incidentu. Významné informační systémy, definovány v § 2 písm. d) výše uvedeného zákona, určuje vyhláška.

6.3 Dotčené subjekty a jejich identifikace

- NBÚ jako ústřední správní úřad působící v problematice kybernetické bezpečnosti;

- Ministerstvo vnitra jako spolupracovník při tvorbě vyhlášky k zákonu o kybernetické bezpečnosti;

- Správci významných informačních systémů - orgány veřejné moci.

6.4 Vyhláška a její cíl

V připomínkovém řízení k zákonu o kybernetické bezpečnosti bylo vydáno odůvodnění, které říká: „*Cílem vyhlášky bylo naplnit zmocňovací ustanovení určené pro Národní bezpečnostní úřad a Ministerstvo vnitra v § 28 odst. 1 zákona o kybernetické bezpečnosti, které slouží k provedení § 6 písm. d) tohoto zákona, tj. především stanovit konkrétní významné informační systémy a jejich určující kritéria, jejichž správci budou podléhat povinnostem podle zákona o kybernetické bezpečnosti. Tímto bude zajištěna vyšší úroveň bezpečnosti informací v těchto informačních systémech. Vyhláška za tímto účelem stanovuje dvojí způsob určení významných informačních systémů. Tím prvým je taxativní výčet významných informačních systémů v příloze č. 1 k této vyhlášce, které zároveň splňují určující kritéria stanovená touto vyhláškou. Druhým způsobem je pak*

samotné určení významného informačního systému jeho správcem, a to na základě výše zmíněných určujících kritérií. Z oblasti významných informačních systémů jsou přímo vyhláškou vyloučeny informační systémy obcí a informační systémy hlavního města Prahy, pokud jsou používané při výkonu jejich vlastní působnosti. Určující kritéria dělí vyhláška na dopadová a oblastní. Dopadová kritéria stanovují nutný následek úplné nebo částečné nefunkčnosti informačního systému způsobené narušením bezpečnosti informací. Zároveň jsou kvantifikována požadovanou dobou výpadku nebo množstvím nákladů nutných pro jejich odvrácení. Dopadová kritéria jsou rovněž nepřímo navázána na kritéria stanovená v nařízení vlády č. 432/2010 Sb., o prvcích kritické infrastruktury, ve znění pozdějších předpisů (dále jen „Nařízení"), kdy následky v nich stanovené nedosáhnou hodnot pro určení prvku kritické infrastruktury podle průřezových kritérií stanovených tímto Nařízením. Oblastní kritéria jsou stanovena v příloze č. 2 k této vyhlášce a mají za cíl určit obecné oblasti činnosti orgánů veřejné moci, na které by se významné informační systémy mohly vázat." (Návrh vyhlášky, 2014)

7 Kritická infrastruktura

Definice kritické infrastruktury říká, že kritickou infrastrukturou se rozumí výrobní a nevýrobní systémy a služby, jejichž nefunkčnost by měla závažný dopad na bezpečnost státu, ekonomiku, veřejnou správu a zabezpečení základních životních potřeb obyvatelstva. Z definice vyplývá, že úkolem společnosti je tedy kritickou infrastrukturu chránit tak, aby fungovala za běžných, mimořádných i krizových situací. Z tohoto je možno vyvodit, že ochrana kritické infrastruktury je proces, který při zohlednění všech rizik a hrozeb směřuje k zajištění fungování kritické infrastruktury. (ŠENOVSKÝ M., 2007)

Na kritickou infrastrukturu musíme pohlížet jako na komplexní systém. Kritická infrastruktura má síťové uspořádání, které se skládá z jednotlivých prvků sítě a spojnic, jednotlivé prvky jsou vzájemně provázané. Stejně jako v každé síti se i zde nachází místa, kde se schází více prvků spojnic, které tvoří uzel. Proto poškození, narušení nebo výpadek některého uzlu má více nebo méně závažný dopad na funkčnost dalších uzlů. Tento výpadek by mohl způsobit následné zhroucení celé kritické infrastruktury. Z tohoto důvodu by mělo být v zájmu ochrany kritické infrastruktury tyto uzly chránit. Ochrana kritické infrastruktury je založena na snížení zranitelnosti systému neboli zvýšení jeho odolnosti vůči dopadům mimořádných událostí. Pro tyto případy je nutné mít připravená opatření zaměřená na zmírnění a odstranění škod. Z toho vyplývá, že se snažíme pomocí provádění preventivních opatření, např. zvýšením bezpečnosti systému technickoorganizačním opatřením, zabránit vzniku mimořádných událostí nebo alespoň udržet následky způsobené mimořádnými událostmi v co nejnižším rozsahu. (ŠENOVSKÝ M., 2007)

Největším problémem v ochraně kritické infrastruktury je fakt, že ne všechny prvky jsou ve vlastnictví státu. Z toho vyplývá, že stát nemůže soukromé subjekty, které tyto prvky vlastní, nutit do investic zvyšující jejich bezpečnost. Pro soukromé subjekty je na prvním místě generování zisku. I přes toto úskalí je nutné, aby se stát problematikou ochrany kritické infrastruktury zabýval, neboť je nutná k zajištění životních potřeb obyvatelstva a státu.

7.1 Prvky kritické informační infrastruktury - ochrana

Kybernetická bezpečnost si klade za cíl ochranu prvků informačních systémů kritické infrastruktury. Tyto systémy jsou nedílnou částí téměř všech kritických infrastruktur. Je nutné zajistit a vytvářet podmínky, aby veřejný i soukromý sektor měl možnost úzce spolupracovat na bázi předávání informací. Bylo diskutováno, kde a zda vůbec budou opatření povinně vyžadována, zda se budou u určitých systémů přijímat pravomoci dodatečně v případě určitých incidentů. (NCKB, 2012)

8 Co je a jak funguje CERT/CSIRT

Problematika kybernetické kriminality se odráží také v budování organizací aktivně se zabývající ochranou a sledováním kyberprostoru. Příkladem může být vznik CERT nebo Computer Security Incident Response Team (dále jen „CSIRT“) týmů a NCKB. Tyto organizace vznikají ve všech vyspělých zemích po celém světě a snaží se definovat obecné fungování, koncepci, působnost, služby a komunikační pravidla, stejně jako legislativní rámec, aby mohly reagovat jako součást krizového řízení při ohrožení státu.

8.1 Computer Security Incident Response Team

CSIRT nebo CERT týmy jsou jedněmi z prvků v boji proti počítačové kriminalitě. Byť jsou tyto zkratky jiné s jiným historickým vývojem, můžeme jejich působnost chápat stejně. Tyto týmy jsou zodpovědné za řešení incidentů v kybernetické oblasti a jsou jakýmsi ústředím, na které se mohou uživatelé či jiné týmy obrátit a žádat o pomoc při řešení nebo podezřením se zjištěným bezpečnostním incidentem.

CSIRT týmy jsou zakládány v rámci organizací poskytujících chod internetu nebo organizací využívající internetové prostředí pro svou hlavní činnost. Povinností CSIRT týmu je kooperace a pomoc při řešení bezpečnostních incidentů, které se bezprostředně dotýkají jejich organizace a v rámci jejich působnosti. Ve své podstatě, každá větší organizace již takový tým provozuje. Rozdílem mezi CSIRT a standartním bezpečnostním týmem je v zapojení do národní nebo světové infrastruktury, kde dochází ke sdílení získaných poznatků s jasně danými standardy a postupy.

Na týmy typu CSIRT jsou kladeny požadavky, které by měl splňovat. Jedná se o deklaraci svých kontaktních údajů, pravidla činnosti, personální složení, informace o možnosti kontaktování, jaké činnosti a služby poskytuje. Dále by takovýto tým měl jasně deklarovat svou působnost, pravomoci a odpovědnost. Na základě těchto údajů může být tým kontaktován a může být nápomocný při řešení problémů, incidentů spadajících do jeho kompetence.

Řešení incidentů může být několik a to především v závislosti na jeho povaze, nastavení týmu a interních předpisech týmu. Řešením může být zneškodnění zdroje prostým odpojením, lokalizace pachatele, obnovení provozu systémů apod. Tyto týmy můžeme dále dělit na interní a koordinační podle činnosti, kterou mají ve své

kompetenci. Interní týmy mohou přímo a aktivně zasahovat v místě incidentu. Týmy koordinační tuto možnost nemají. Jejich přínosem je komunikace, spolupráce a sdílení informací o daném incidentu.

Pokud dojde k bezpečnostnímu incidentu, snaží se jej vyřešit účastníci přímo u zdroje nebo u cíle. V podstatě se může stát, že zdroj útoku i cíl útoku spadá do kompetence jednoho CSIRT týmu. To je ovšem ideální stav, kdy nedochází k prodlení při předávání informací a daný tým může efektivně zasáhnout za pomoci odborníka v místě. Problém nastává, když oběť útoku nedovede zdroj identifikovat. Příčiny mohou být různé, zdroj o sobě při útoku nedává žádné informace, nereaguje nebo jen odmítá problém řešit. V této fázi by měl nastoupit vládní, národní tým.

8.2 Národní a vládní CSIRT týmy

Národní a vládní CSIRT týmy jsou typem koordinačním. Jejich funkce spočívá ve zprostředkování kontaktů v rámci své oblasti mezi napadeným a původcem, pokud je znám. Vládní a národní CSIRT týmy nedisponují a nespravují fyzicky informační a komunikační infrastrukturu, tudíž nemohou, v místě incidentu, přímo zasahovat. Poskytnou potřebné kontakty a koordinují postupy při řešení problému, jehož řešení si žádá spolupráci více složek.

Z nastavení struktury a fungování SCIRT týmů plyne pro vládní či národní týmy jen minimum incidentů. Valná většina je řešena přímou komunikací mezi dotčenými stranami bez nutnosti žádat o řešení vládní nebo národní CSIRT. Národní a vládní týmy řeší velmi závažné či opakované incidenty, které odmítají řešit odpovědné osoby, nebo nelze jednoznačně určit, kdo je za jejich řešení odpovědný.

Národní tým CSIRT má ve své gesci spolupráci, osvětu a vzdělávání veřejnosti. Pomáhá zakládat a podporuje vznikající podnikové CSIRT týmy. Uvádí je do problematiky a poskytuje již zavedené standardy, postupy a procedury. Tím rozšiřuje transparentnost celého prostředí a poskytuje poškozeným možnost rychlého uvedení do původního stavu.

Vládní tým CSIRT je odrazem národního týmu, ovšem se zaměřením na státní správu a samosprávu. Má v gesci problematiku, která ohrožuje kybernetickou

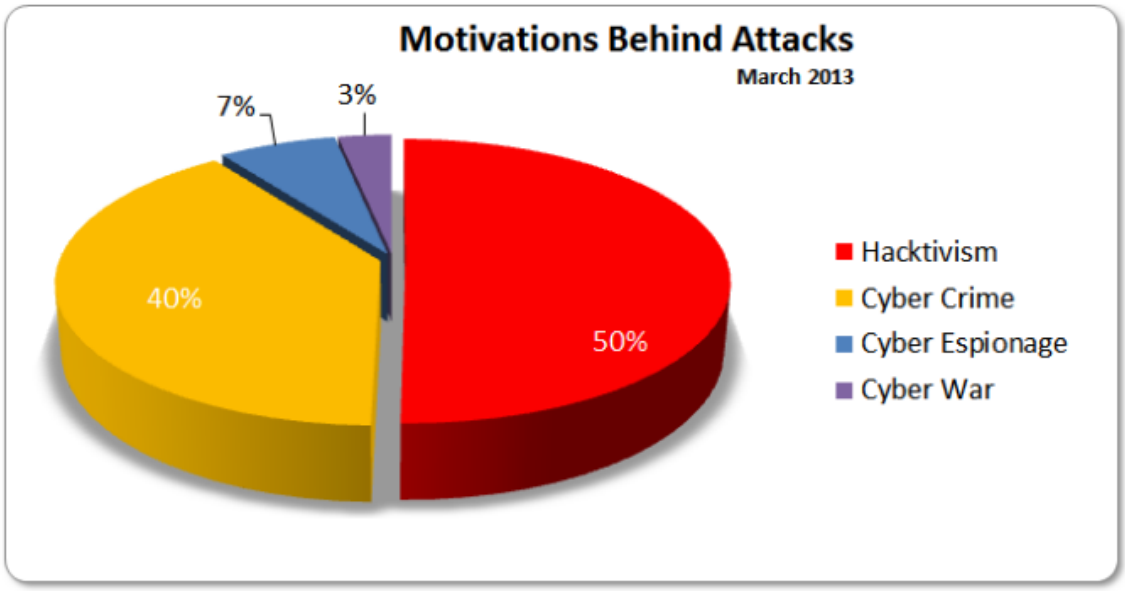
bezpečnost státu. Vládní tým může mít podobu interní i koordinační. Pokud se jedná o podobu interní, jsou jeho pravomoci a odpovědnost podložena legislativou.

9 Vybrané případy

V dalších kapitolách se budu věnovat skutečným případům, na kterých bych rád demonstroval reálné hrozby, jak byly zaznamenány v čase. Zdrojem pro získávání informací jsem si zvolil zahraniční servery specializované na danou tématiku. Jedná se o servery hackmageddon.com, zdnet.com, root.cz, ibtimes.co.uk, phys.org thehackernews.com, cnet.com apod. Vzhledem k rozsáhlosti dané tématiky jsem se zaměřil na jeden případ z roku 2011, kdy se spojily dvě skupiny hackerů a vnikla tak operace nazvaná AntiSec. Jednotlivé útoky analyzuji z pohledu akce a reakce, abych nalezl možnou souvislost v reakční době na daný podnět.

Česká republika zaznamenala největší kybernetické útoky v březnu 2013. Na obrázcích ze serveru hackmageddon.com jsou patrné útoky v celosvětovém měřítku z tohoto měsíce a roku.

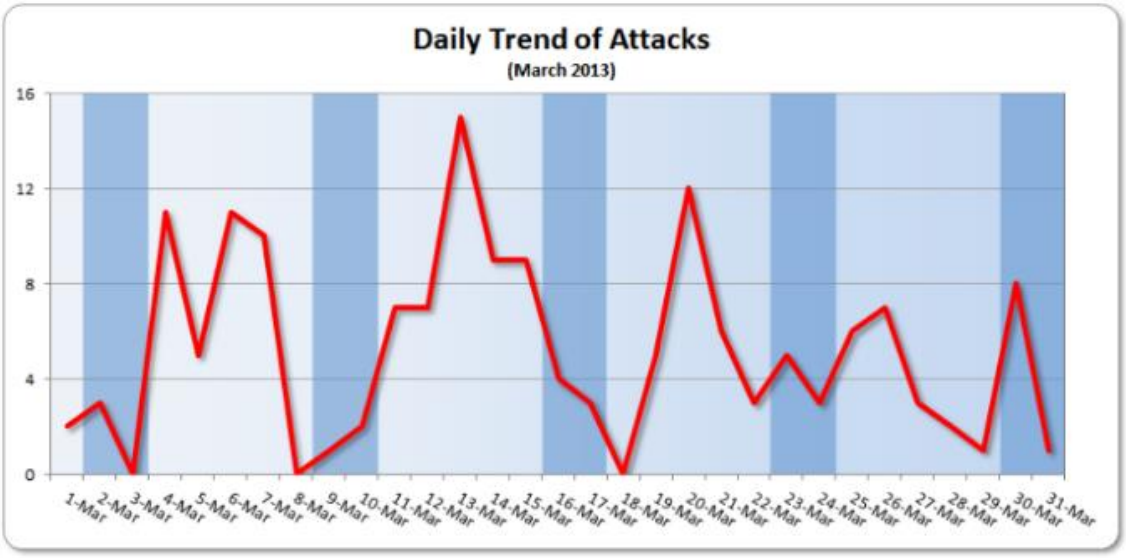
Graf č. 2 – Motivace útoků



Zdroj: http://hackmageddon.com/

Z tohoto grafu je patrný poměr mezi jednotlivými útoky. Převažuje hacktivizmus následovaný kybernetickou kriminalitou. V malém, nikoliv zanedbatelném, zastoupení je kybernetická špionáž a kybernetická válka.

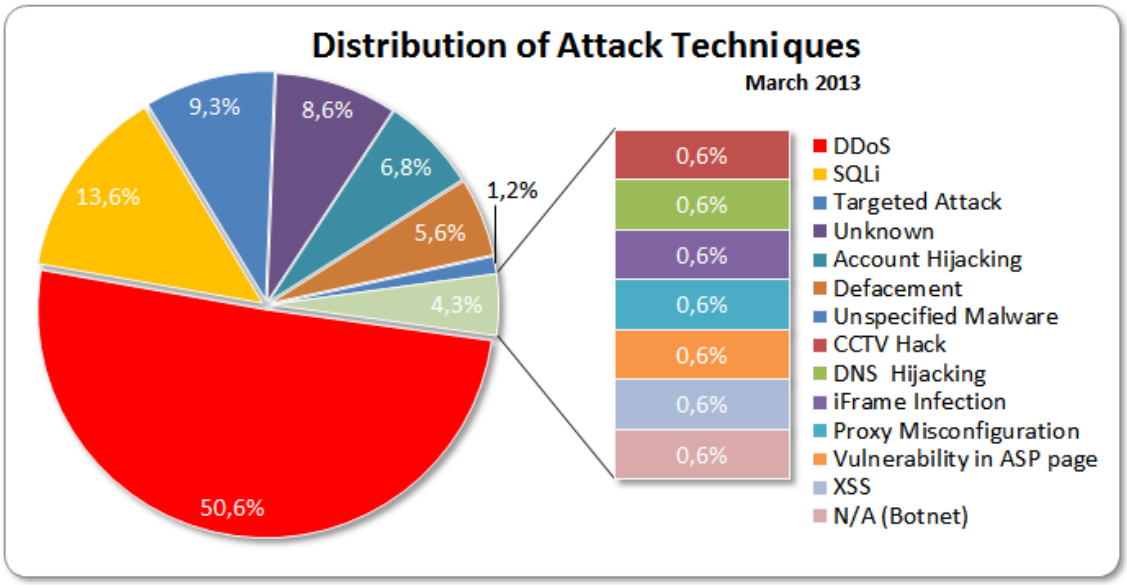
Graf č. 3 – Denní trend útoků



Zdroj: http://hackmageddon.com/

Tento graf znázorňuje jednotlivé dny, tak jak byly útoky zaznamenány a odhaleny. Z našeho pohledu je zajímavý 4. a 7. březen. V celosvětovém měřítku se útoky na Českou republiku projevily takovýmto nárůstem.

Graf č. 3 – Techniky útoků



Zdroj: http://hackmageddon.com/

Z tohoto grafu jsou patrné typy útoků. Více než polovinou převažuje útok typu DDoS.

10 Vybrané kybernetické hrozby

Jak jsem již výše avizoval, zaměřím se na operaci AntiSec, ke které se ve většině případů hlásily hackerské skupiny Anonymous a Lulz Security. Pojem hackerská skupina začal vznikat v 80. letech 20. století společně s nástupem domácích počítačů. Termín hacker byl původně spojen s jakýmkoliv počítačovým nadšencem. Později se tento termín začal používat v negativním slova smyslu pro uživatele počítačů, kteří jej měli jako nástroj k nelegální činnosti. Sdružováním jednotlivých uživatelů vznikaly hackerské skupiny.

10.1 Hackerká skupina Anonymous

Skupina Anonymous (zkráceně Anon) je nadnárodní skupinu označovanou jako nezávislé sdružení hackerů, recesistů a síťových aktivistů. Anonymous je, jak již název napovídá, anonymní hnutí, bez vnitřní struktury. Cíl této skupiny není příliš zřejmý, stejně tak i proti komu nebo čemu bojuje. Jejich aktivita je nejvíce patrná v kybernetickém prostoru, kde atakují různé stránky, za což jsou vnímáni jako hackeři. Dále se tato skupina projevuje různými žerty a reakcemi na činy politiků nebo jiných mediálně se projevujících osob. Vyjadřují tím svůj protest a nesouhlas. Jejich projevy jsou anonymní, bez uvedení autora, pouze s odkazem na skupinu Anonymous. Tato nadnárodní skupina má své příznivce a členy i v České republice. Nejčastější metodou používanou je tzv. DDoS útok, který zahltí požadavky cílový server, až do kolapsu. (Novinky, 2015) Jedná se o velmi aktivní a známou hackerskou skupinu. O tom, jak je skupina Anonymous mezinárodně rozsáhlá, aktivní a populární svědčí například informace z června roku 2012, kdy německá policie identifikovala 106 počítačových uživatelů podezřelých ze spolupráce s touto hackerskou skupinou. (WeltN24, 2015)

Dalším příkladem bych mohl uvést pochod uskutečněný na protest k prvnímu výročí projektu Occupy Wall Street, pořádaný skupinou Anonymous. Během pochodu bylo v New Yorku zatčeno skoro 200 lidí. (KAZMI, 2011) Jedná se pouze o náhodně vybrané příklady, kterými chci nastínit působnost skupiny Anonymous.

10.2 Hackerská skupina Lulz Security

Další neméně významnou skupinou působící v kyberprostoru byla skupina Lulz Security. I tato skupina byla nadnárodní, nezávislá. Její jméno vzniklo ze zkratky LOL (Laughing Out Loud - v překladu smát se nahlas) toto odkazuje na jejich tvrzení, že vše činí pro zesměšnění svých obětí a ne pro finanční profit. V logu této skupiny je muž s knírkem, cylindrem a monoklem. Lulz Security se zabývala vyhledáváním nechráněných nebo nedostatečně chráněných internetových stránek, z nichž pak stahovala citlivé informace, které následně zveřejňovala. Nejvíce známe útoky, za kterými Lulz Security stála, jsou na společnost Nintendo, Sony a Fox. Její oficiální působení trvalo pouze 50 dní, známé jako 50 days of Lulz. Nicméně jednotliví členové této skupiny působili dále. Lídrem skupiny byl Hector Xavier Montsegurzvaný jako Sabu. (MOOS, 2012)

V roce 2012 byly uveřejněny informace, že Hector Xavier Montsegurjiž půl roku spolupracuje s FBI a pomáhal se zatýkáním dalších členů Lulz Security a Anonymous. (MOOS, 2012)

Tyto skupiny zmiňuji, neboť bych se rád zaměřil na operaci Antisec, kterou organizovaly skupiny Lulz Security a Anonymous. Vyhlásily tzv. „okamžitou a trvalou válku všem svobodu-ohrožujícím moderátorům“ (OLSONOVÁ, 2012).

10.3 AntiSec opreace

Operace Anti-Security (AntiSec), je pojem, který můžeme přeložit jako „protibezpečnost“ nebo proti bezpečnosti. Výše zmiňované skupiny LulzSec a Anonymous uveřejnily v červnu 2011 informaci o svém spojení v operaci AntiSec. Tato operace si kladla za cíl napadat mezinárodní vládní a finanční instituce, které omezují svobodu projevu a svobodu internetu. Ve svém prohlášení vyzývaly kohokoliv, kdo je schopen a ochoten napadat webové stránky organizací a zanechání v jejich HTML kódu pojem AntiSec. Plné znění tohoto prohlášení viz příloha č. 1.

Operace AntiSec proběhla během 4 měsíců od června do září roku 2011. V průběhu této operace bylo provedeno celkem 33 akcí.

10.4 Akce realizované v rámci operace Antisec

První akce spadající do operace Antisec byla realizována 20. června 2011. Jednalo se o DDoS útoky na internetové stránky SOCA (Serious Organised Crime Agency) zabývající se počítačovou kriminalitou. Souběžně s touto akcí byl realizován útok na čínskou síť, konkrétně na vládní www.jhq.gov.cn. V těchto případech se útočníci přihlásili ke skupině LulzSec. Následky: Jelikož se jednalo o DDoS útoky, došlo k znepřístupnění internetových stránek.

Dalšími DDoS útoky byly 22. června napadeny vládní stránky Brazílie. Jednalo se o www.receita.fazenda.gov.br, www.presidencia.gov.br a www.portalbrasil.gov.br. Stránky byly zahlceny a nepřístupné dvě a půl hodiny. Tentýž den byl realizován útok na internetové stránky www.petrobras.com.br. Jednalo se o portál největší brazilské energetické společnosti PETROBRAS. (MCMILLAN, 2011) Po odeznění tohoto útoku, následoval další, který cílil na uživatelské účty zaměstnanců společnosti PETROBRAS. Brazilská odnož skupiny LulzSec na svém twitterovém účtu několik hodin zveřejňovala odkaz na server PETROBRASu, včetně přístupových kódů. (RAPOZA, 2011) K těmto útokům se přihlásila brazilská odnož LulzSec. Následky: Jelikož se jednalo o DDoS útoky, došlo k znepřístupnění internetových stránek. V druhém případě hrozila kompromitace zaměstnaneckých účtů a citlivých údajů.

Útokům ve čtvrtek 23. června čelily internetové stránky policie v americké Arizoně http://www.azdps.gov/. Skupina LulzSec uvedla, že získala soubory, které se týkaly státní hranice, zpravodajských bulletinů, výcvikových příruček, osobních e-mailových korespondencí, jmen, telefonních čísel, adres a hesel sloužících k vymáhání práva ve státě Arizona. Zveřejněno bylo cca 500 MB dat. Útok byl odpovědí na migrační zákon a rasovou profilaci místní policie. (TSOTSIS, 2011) Dokumenty, které byly uveřejněny v roce 2011, jsou stále k dispozici a lze je stáhnout prostřednictvím služby Torrent. Následky: Zveřejněním výše uvedených údajů mohlo mít za následek dočasnou paralyzaci policejní činnosti v dané oblasti.

24. června se pod hlavičkou operace AntiSec nabourala skupina Anonymous do serverů Columbian "Black Eagles" a zveřejnila jména 2800 členů. Jedná se kolumbijské speciální jednotky. Útok byl veden na tento server, neboť se jednalo údajně o zkorumpovanou policejní jednotku zapojenou do obchodu s drogami, vydírání a únosů

osob. (TIMES, 2011) Následky: Došlo ke kompromitaci citlivých údajů členů policejní jednotky, a tím k jejich ohrožení, případně k ohrožení členů jejich rodin.

Dne 25. června uveřejnila Skupina Lulz Security na svých stránkách a na stránkách Pirate Bay zprávu o ukončení své 50 - ti denní činnosti, zvanou jako 50 days of Lulz.V této zprávě byly obsaženy informace získané během své avizované činnosti, nejen během operace AntiSec. Jednalo se konkrétně o IP adresy, e-maily, hesla uživatelů různých herních i státních portálů. Konečná zpráva tak obsahovala velké množství citlivých dat. Na základě této zprávy se dalo předpokládat, že Lulz Security ukončila svou činnost. Nicméně, ne všichni členové této skupiny svou činnost ukončili a pokračovali společně s hnutím Anonymous v operaci AntiSec.

To se potvrdilo v noci na 27. června, kdy hackeři z Anonymous zveřejnili na svých stránkách informace stažené ze serverů National Education Laboratory, Cyberterrorism Defence Initiative´s Security a Network Training Initiative. Dále zveřejnili informace amerického vzdělávacího programu Sentinel zabývající se vnitřní bezpečností, informacemi o softwarových nástrojích hackerů. (REISINGER, 2011) Následky: Zveřejněním těchto informací mohlo dojít k paralyzaci nebo omezení funkčnosti výše zmiňovaných agentur.

28. června byly napadeny stránky Tuniské vlády. Tyto stránky zobrazovaly po dobu útoku znak skupiny Anonymous. Stránky byly jinak funkční. (GAYATHRI, 2011) Následky: Nejednalo se o útok, který by významným způsobem poškozoval obsah webu. Tento útok si kladl za cíl zviditelnění hackerů a skupiny Anonymous a upozornění na cenzu internetu v Tunisu.

Na twitterovém účtu Anonymous byly 29. června zveřejněny další informace, které byly získány 23. června ze stránek arizonské policie. Tentokrát byla zveřejněna jména, adresy, telefonní čísla, hesla, čísla sociálního pojištění, hlasové zprávy, chat logy. (ALBANESIUS, 2011) Následky: Jednalo se o citlivá data a soukromou komunikaci příslušníků policie, které mohly mít dopad na jejich soukromý i profesní život.

30. června skupina Anonymous společně s LulzSec pod hlavičkou operace AntiSec napadly a zveřejnily informace ze stránek společnosti Viacom a Universal Music

Group, které označovali jako zkorumpované. Zveřejněna byla hesla a vnitřní struktura serverů. Současně s těmito informacemi byla zveřejněna i data z vládních stránek Zimbabwe, kterými chtěli útočníci poukázat na neprůhledné volby prezidenta Roberta Mugabe v roce 2008. Dále byly zveřejněny informace z vládních stránek Austrálie a Brazílie. Australská vláda vydala prohlášení, kterým dementovala prolomení svého zabezpečení, neboť informace uváděné ve zprávě Anonymous jsou volně dostupné. Na stránkách brazilské vlády bylo vystaveno video, které kritizovalo manipulaci s informacemi. Těmito útoky chtěli upozornit na nedostatek informací ze stran vlád a tím na omezení demokratického zřízení. (ALBANESIUS, 2011) Následky: Byly kompromitovány citlivé údaje společností Viacom a Universal Music Group, které mohly být následně zneužity.

1. července skupina AntiSec oznámila další úspěšný útok na webové stránky policejního oddělení v Arizoně. Tento útok byl realizovaný na základě předchozích útoků, kdy byly získány e-mailové zprávy s rasovou tématikou namířenou proti muslimské komunitě. Útok byl veden pomocí DDoS a zapříčinil vyřazení serverů, které byly nedostupné. Ve své zprávě útočníci uvedli, cituji: „*Let this third and crushing blow against Arizona police send a strong message to the ruling class around the world," reps for Anonymous trumpeted on Pastebin, a website where the people can upload messages or code. "You will no longer be able to operate your campaign of terror against immigrants and working people in secrecy: we will find you, expose you, and knock you off the internet. Many lulz have been had while we purposefully strung you along slowly and painfully for the past two weeks.“* (SHAER, 2011) Následky: Vyřazením serverů nebylo možno stránky policie zobrazit a tím byl znemožněn přístup potencionálním návštěvníkům.

Další akcí, ke které se přihlásili přívrženci LulzSec a Anonymous pod hlavičkou AntiSec bylo napadení stránek Orange Country. Jednalo se o politickou stranu demokratů, působících na americké Floridě. Staženy a zveřejněny byly seznamy členů této strany. Útok byl součástí operace Orlando vedené pouze skupinou Anonymous. Jednalo se o reakci na zatýkání aktivistů "Food Not Bombs", kteří rozdávali potraviny bezdomovcům. (WILSON, 2011) Následky: Zveřejněním seznamu členů politické strany mohlo mít dopad na jejich soukromý i profesní život.

Obětí útoku se 3. července staly stránky společnosti Apple, ze kterých byly získány informace k 26 uživatelským účtům. Jména a hesla těchto účtů byly zveřejněny na twitterovém účtu AntiSec. Ke zveřejněným informacím bylo připsáno, že AntiSec objevila chybu v zabezpečení systému a může tak získávat informace k dalším účtům vedených u společnosti Apple. (MAITY, 2011) Následky: Zveřejněním těchto informací byl ohrožen prodej nových zařízení společnosti Apple a tím i snížení zisků uvedené společnosti.

4. července se do operace AntiSec připojila skupina s názvem Script Kiddies. Tato skupina napadla účet na Twitteru televizní společnosti Fox News. Jménem společnosti pak zveřejňovala informace o zavraždění prezidenta Baracka Obamy. (READ, 2011) Stejná skupina dále napadla účet na Twitteru a Facebooku společnosti Pfizer, zabývající se léčivy. Na těchto účtech následně zveřejňoval nepravdivé informace. Script Kiddies uváděla, že přístup k účtům byl nedostatečně zabezpečen a k jeho kompromitaci stačilo zadat jméno jednoho ze zaměstnanců společnosti Pfizer. (BREWSTER, 2011) Následky: Zveřejňováním nepravdivých informací docházelo ke zmatení či přímo ke klamání uživatelů, kteří dané stránky sledovali.

4. července byl na stránkách The Pirate Bay uveřejněn soubor o velikosti 600 MB, který obsahoval volební výsledky jednoho z okrsků v Austrálii. Soubor na stránky umístila osoba s pseudonymem „f1esc“ hlásící se k operaci AntiSec. Australské úřady vydaly prohlášení, že uvedená data nejsou citlivá a lze k nim veřejně přistupovat prostřednictvím FTP serveru a to už od března 2011. (CHIRGWIN, 2011) Následky: Vzhledem ke skutečnosti, že se jednalo o veřejně dostupné informace, byly následky nulové.

V rámci operace AntiSec se 5. července k útoku na stránky turecké vlády přihlásila skupina hackerů z RedHack. Vyřazení vládních serverů bylo protestem proti cenzuře tureckého internetu a připomenutím výročí úmrtí 35 intelektuálů zavražděných 2. července 1993 davem radikálních islamistů. (STEVENSON, 2011) Následky: Vyřazením serverů bylo zamezeno potenciálním uživatelům získávat informace.

Italské bezpečnostní složky zatkly 15 osob, které označily za příslušníky skupiny Anonymous odpovědné za DDoS útoky na vládní i soukromé servery. Odpovědí na toto

zatýkání bylo prohlášení o pomstě. Takto byla označena zveřejněná data získaná z italských univerzit a společnosti Nimbuzz, která byla poskytovatelem VoIP telefonie. Tato společnost byla vybrána k útokům na základě svého prohlášení o spolupráci s vládními úřady na blokaci přístupu k jeho službám a to s aktivním přístupem bez požadavků, což je podle Anonymous nepřijatelná cenzura. (BRIGHT, 2011) Následky: Došlo k narušení soukromí zaměstnanců a žáků univerzit a interních dokumentů s citlivými údaji společnosti Nimbuzz.

6. července se skupina Anonymous připojila a tím i podpořila aktivitu hackerů z RedHack tím, že na 74 vládních stránkách v Turecku editovala jejich obsah. Tuto akci nazvali „Turkish Takedown Thursday“ Došlo k znepřístupnění části serverů a v ostatních případech ke změně obsahu. Tyto informace zveřejnilo na svém twitterovém účtu Anonymous s odkazen na operaci AntiSec. (STEVENSON, 2011) Následky: Dezinformace veřejnosti a nemožnost na stránky přistupovat.

Zvláštním případem bylo napadení a zveřejnění uživatelských jmen, hesel a e-mailových adres na serveru PasteBin hackerem s přezdívkou P0keu 6. července. Informace byly získány ze serveru tamilcanadian.com. Uživatel P0keu ke zveřejněným informacím sice uvedl, že je získal v rámci operace AntiSec, nicméně již neuvedl důvod, proč si vybral tento zpravodajský webový server. (WILSON, 2011) Následky: Kompromitace uživatelský přístupů, které mohlo následně vézt k jejich zneužití.

Dalším neméně závažným útokem skupiny Anonymous pod hlavičkou AntiSec bylo napadení a následné zveřejnění interních dokumentů, e-mailové komunikace a vývojových schémat společnosti IRC, která je významným dodavatelem IT technologií pro americké federální úřady. Společnost IRC byla napadena pro její kooperaci s úřady na projektu SIM (Special Identities Modernization) zabývající se snižováním teroristických a kriminálních aktivit. (KUMAR, 2011) Následky: Zveřejnění těchto informací může mít fatální důsledky, neboť mohl dojít ke kompromitaci strategie v boji proti terorismu.

Operace AntiSec pokračovala i 11. července napadením stránek amerického ministerstva obrany a vnitřní bezpečnosti, ze kterých bylo staženo a následně zveřejněno 67 tis. unikátních e-mailových adres. 53 tis. těchto adres bylo registrováno

v doméně *.mil (doména *.mil je výhradně rezervována pro ozbrojené síly USA). Ostatní e-mailové adresy patřily dodavatelům spolupracujícím s těmito institucemi. (JIJO, 2011) Následky: Zveřejněním e-mailových kontaktů bylo ohroženo soukromí jednotlivých uživatelů a kompromitace dodavatelů a spolupracovníků bezpečnostních složek.

12. července byly napadeny stránky potravinářské společnosti Monsanto skupinou Anonymous. Získány byly informace o 2,5 tis. zaměstnancích a spolupracujících osobách. Informace, uveřejněné na twitterovém účtu AntiSec, obsahovaly telefonní čísla, adresy a jména. Tento útok byl veden pro údajnou zkorumpovanost společnosti a její neetické obchodní aktivity. (PAULI, 2011) Následky: Kompromitace uživatelský přístupů mohla vézt k jejich zneužití.

14. července se podruhé zviditelnil hacker s přezdívkou p0ke, který se odvolával na operaci AntiSec, když zveřejnil na serveru Pastebin informace získané ze společnosti Stevens Institute of Technology sídlící v New Jersey. Kompromitována byla hesla a uživatelská jména společně s e-mailovými adresami, které byly uloženy v databázi této společnosti. (KUMAR, 2011) Následky: Kompromitace uživatelských přístupů, které mohlo následně vézt k jejich zneužití.

Přestože, LulzSecurity oznámila 25. června ukončení své činnosti, přihlásila se v rámci operace AntiSec k pozměnění a přesměrování webových stránek časopisu The Sun. Na těchto stránkách uveřejnili zprávu o úmrtí Keitha Ruperta Murdocha (miliardář a mediální magnát). Po vypršení časového limitu došlo k přesměrování na twitterový účet Lulz Security. Okamžitě po zjištění, že byly stránky The Sun pozměněny, došlo k vyřazení i stránek News International, které Keith Rupert Murdoch provozoval. Později bylo vydáno prohlášení, že odpojení stránek bylo záměrné a z preventivních důvodů. (ARTHUR, a další, 2011) Následky: Klamání veřejnosti, ztráta důvěry v časopis The Sun. Preventivní vypnutí stránek News International spojené se ztrátou příjmů.

19. a 20. července byly uveřejněny informace o zadržení 16 osob podezřelých z kybernetických útoků. Čtyři osoby byly zadrženy na území Holandska, které se hlásily k odnoži Anti Security NL. Tyto osoby byly odpovědné za napadení stránek společnosti

Nimbuzz (viz výše) a stránek pepper.nl. (MENN, 2011) Následky: Zveřejněním citlivých údajů byly poškozeny obě uvedené společnosti.

V rámci probíhající operace AntiSec uveřejnila skupina Anonymous 21. července na stránkách Twitteru informace o získání 1GB dat ze serverů NATO. Z celého množství uveřejnily pouze dva dokumenty ve formátu PDF. První dokument byl datován do roku 2007 a obsahoval informace o řídícím centru ISAF v Afghánistánu. Druhý dokument byl datován do roku 2008 a týkal se mise v Kosovu. (STEVENSON, 2011) Následky: Jelikož se útočníci rozhodli nezveřejnit získaná data, byly následky relativně malé. Za předpokladu, že by došlo ke zveřejnění veškerých získaných dat, lze jen těžko odhadnout, jaké následky by toto odhalení mělo. Obecně lze říci, že kompromitace materiálů NATO jsou velmi citlivé a mohly by se dotýkat členských států, či konkrétních osob.

Příznivci skupiny Anonymos z Rakouska atakovali stránky agentury Gebuhren Info Service, přes které získali přístupy k bankovním údajům bezmála 100 tis. klientů. Únik těchto údajů byl avizován a jednotliví klienti byli vyzváni ke změně přihlašovacích údajů. Získané informace nebyly hackery zveřejněny. Dalším útokem rakouských Anonymous byla napadena extrémně pravicová strana Svobody a strana sociálních demokratů. (AFP, 2011) Následky: Potenciálním zveřejněním přístupových údajů k bankovním účtům by znamenalo poškození velkého množství klientů a velkou finanční ztrátu.

Italská odnož Anonymous zveřejnila informace italských jednotek boje proti počítačové kriminalitě Centro Nazionale Anticrimmine Iformatico per la Protezione delle Infrastrutture Protection. Na twitterových stránkách AntiSec tvrdili, že disponují více než 8 GB dat této organizace. Zveřejněno bylo pouze 100 MB. (TELEGTAPH, 2011) Následky: Zveřejněním byť jen části informací byla ohrožena funkčnost celé organizace.

26. července byly uveřejněny informace o kybernetických útocích na vládní stránky Kolumbie, Peru a Filipín. Útoky byly vedeny pod hlavičkou operace AntiSec a zaměřily se na osobní údaje státních zaměstnanců policie a vlády. Získané informace byly následně zveřejněny na serveru Pastebin. (STEVENSON, 2011) Následky: Došlo ke

kompromitaci osobních údajů státních zaměstnanců a zaměstnanců policie což mohlo mít vliv na jejich soukromý a profesní život.

Jako Fuck FBI Friday III byl označen pátek 29. července, kdy Anonymous zveřejnila 390 MB dat komunikace mezi NATO a americkou armádou. Napadeny byly stránky společnosti ManTech spolupracující s FBI. Tato akce pod hlavičkou AntiSec byla pravděpodobně odvetou za zatýkání členů LulzSec z 19. a 20. července. (GREENBERG, 2011) Následky: Ohrožení dodavatelů technologií FBI a jejich bezpečnosti.

Shooting Sheriffs Saturday Release byla označená akce, která proběhla 31. července. Cílem byly bezpečnostní úřady, ze kterých bylo staženo a zveřejněno 10 GB dat. Tato data obsahovala soukromé e-mailové zprávy, hesla, data o informátorech, školící soubory, čísla sociálních pojištění a informace z kreditní karty jednoho z šerifů. Útok byl odvetou za zatčení a obvinění několika hackerů. (MILLS, 2011) Následky: Došlo ke kompromitaci osobních údajů státních zaměstnanců a zaměstnanců policie což mohlo mít vliv na jejich soukromý a profesní život. Ohrožení policejních informátorů.

16. srpna zveřejnili hackeři hlásící se k AntiSec, 1GB dat soukromých dokumentů patřící společnosti Vanguard Defense Industries. Konkrétně Richardu T. Garciovi viceprezidentovi této společnost, který mimo jiné v minulosti pracoval jako asistent ředitele FBI. Tato společnost se zabývá obranným průmyslem. Zveřejněny byly soukromé poznámky z jednání, smlouvy, schémata, osobní údaje a další dokumenty, které byly označeny „pouze pro interní účely“ a „citlivé“. (SKILLINGS, 2011) Následky: Kompromitací citlivých údajů mohlo dojít k poškození společnosti a případným ekonomickým ztrátám. Stejně tak i k poškození soukromého a profesního života Richarda T. Garcia

Na stránkách Pastebin, MediaFire a Twitteru zveřejnil 24. srpna hacker pod pseudonymem ThEhAcKeR12 citlivé informace ze serveru allianceforbiz.com. Tato stránka patřila společnosti pořádající veletrhy, výstavy a konference s vojenskou tématikou. Zveřejněno bylo 20 tis. záznamů o osobách a firmách, které se těchto akcí účastnily. Jednalo se o uživatelská jména, hesla a e-mailové adresy. (KUMAR, 2011) Následky: Kompromitace jednotlivých účastníků jak osob, tak firem zabývajících se vojenskou problematikou mohlo ovlivnit jejich soukromý i profesní život.

Poslední zaznamenanou akcí vedenou v rámci operace AntiSec byl 1. září útok na webovou stránku provozovanou texaskou policií v USA. K tomuto útoku se přihlásila skupina Anonymous a jednalo se o odvetu za zatýkání údajných členů skupiny Anonymous a LulzSec ve Velké Británii a USA. Po útoku byly zveřejněny jmenné seznamy policejních ředitelů, jejich e-mailové adresy a citlivá data. Mimo jiné byla tato stránka cca tři hodiny nedostupná. (WARWICK, 2011) Následky: Došlo ke kompromitaci osobních údajů zaměstnanců policie, což mohlo mít vliv na jejich soukromý a profesní život. Nedostupnost serveru zamezilo potenciálním uživatelům získávat informace.

Následující tabulka shrnuje jednotlivé útoky a jejich motivaci, kde jsem se zároveň snažil nastínit i časovou prodlevu mezi impulzem a realizací útoku. Některé z útoků mají jasně ohraničené datum a nenesou se tak v duchu operace AntiSec, která se odkazuje na poukazování významných zranitelností na webových stránkách vládních úřadů a firem. Jednalo se zároveň o útoky zviditelňující konkrétní útočníky nebo sledující konkrétní zájem.

Tabulka č. 1 – Výpis jednotlivých útoků

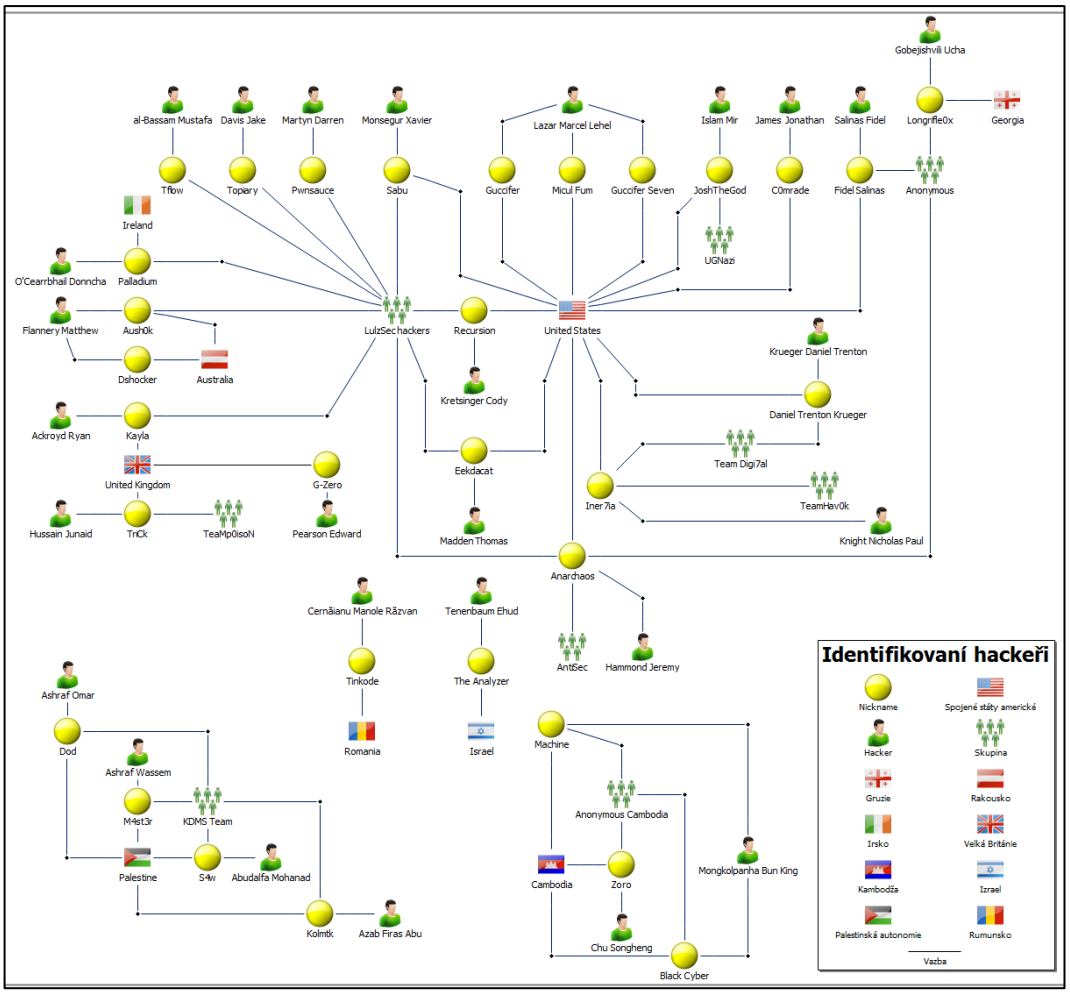
Cíl útoku	**Podnět útoku**		**Realizace / zveřejnění**	**Typ útoku**
	Impuls	**Dne**	**Dne**	
SOCA	Vyšetřování, LulzSec tweeted	13.6.2011	20.6.2011	DDoS
PETROBRAS	Reakce na cenu paliv	2010	22.6.2011	DDoS; Hacktivismus
Policie Arizona	Migrační zákon	29.7.2010	23.6.2011	Hacktivismus
Kolumbijská policie	Polovojenská skupina	N/A	24.6.2011	Hacktivismus
SONY FOX / Vládní servery	Ukončení činnosti LulzSec	N/A	25.6.2011	Hacktivismus
USA bezpečnostní servery	Program proti kybernetické kriminalitě	N/A	27.6.2011	Hacktivismus
Tuniská vláda	Cenzura internetu	2007	28.6.2011	Hacktivismus
Policie Arizona	Migrační zákon	29.7.2010	29.6.2011	Hacktivismus
Zimbabwe vláda	Volby Mugabe	2008	30.6.2011	Hacktivismus
Policie Arizona	Migrační zákon	29.7.2010	1.7.2011	DDoS; Hacktivismus
USA Orlando	Zatýkání aktivistů Food Not Bombs	3.6.2011	2.7.2011	Hacktivismus
Apple	Chyba v zabezpečení serveru	N/A	3.7.2011	Hacktivismus

Fox news	Chyba v zabezpečení Twitterového účtu	N/A	4.7.2011	Hacktivismus
Australké volby	Navrhovaná cenzura internetu	2011	4.7.2011	Hacktivismus
Turecká vláda	Cenzura internetu / výročí vražd	2.7.1993	5.7.2011	DDoS
Nimbuzz	Cenzura služeb VOIP v různých zemích	1.7.2011	5.7.2011	Hacktivismus
Turecká vláda	Cenzura internetu / výročí vražd	2.7.1993	6.7.2011	Hacktivismus
TAMILCANADIAN.COM	Chyba v zabezpečení serveru	N/A	6.7.2011	Hacktivismus
USA společnost IRC	Projekt "Special Identities Modernization"	2011	7.7.2011	Hacktivismus
USA stránky obrany	Projekt "Special Identities Modernization"	2011	11.7.2011	Hacktivismus
Monsanto	Žaloba - modifikované potraviny	N/A	12.7.2011	Hacktivismus
USA Stevens Institute of Technology	Chyba v zabezpečení serveru	N/A	14.7.2011	Hacktivismus
The Sun	Nevlivňování případu s hackery	7.2011	15.7.2011	Hacktivismus
NATO	Zatýkání hackerů	7.2011	21.7.2011	Hacktivismus
Gebuhren Info	Chyba v zabezpečení serveru	N/A	22.7.2011	Hacktivismus
Italské bezpečnostní úřady	Chyba v zabezpečení serveru	N/A	23.7.2011	Hacktivismus
Kolumbie, Peru Filipíny vládní stránky	Chyba v zabezpečení serveru	N/A	26.7.2011	Hacktivismus
NATO x USA	Zatčení hackerů	19.7.2011	29.7.2011	Hacktivismus
USA policieShooting Sheriffs	Zatčení hackerů	7.2011	31.7.2011	Hacktivismus
Vanguard Defense Industries	Vytvoření vojenského dronu - spolupráce s FBI	1.7.2011	16.8.2011	Hacktivismus
USA allianceforbiz.com	Chyba v zabezpečení serveru	N/A	24.8.2011	Hacktivismus
Texas policie	Zatčení hackerů	7.2011	1.9.2011	DDoS; Hacktivismus

Zdroj: vlastní zpracování autora

Následující diagram znázorňuje identifikované hackery, jejich pseudonymy k jaké skupině se hlásí a z jaké země pochází. Diagram byl vytvořen pomocí kontextové analýzy a extrakcí entit z dostupných otevřených zdrojů.

Graf č. 4 – Vazby hackerů ke skupinám



Zdroj: vlastní zpracování autora

Výše popsané útoky byly vedeny v rámci operace AntiSec a nedotýkaly se přímo České republiky. Nicméně v březnu 2013 čelila Česká republika útokům podobného typu (DDoS). Následkem bylo znepřístupnění zpravodajských serverů a serverů některých bankovních institucí. Z toho vyplývá, že Česká republika nestojí stranou a je nutné s kybernetickými útoky počítat a být na ně připraveni.

11 Diskuze

Při úvaze o bakalářské práci jsem vycházel ze svého zájmu o kybernetickou bezpečnost a z faktu, že již patnáct let pracuji na NBÚ jako analytik otevřených zdrojů. Bylo pro mě výzvou zjistit, zda je možné dohledat a v závěru zhodnotit vybraný časový úsek, ve kterém vybraná skupina osob útočila na předem vybraný cíl.

Jako první mne napadla myšlenka, zda každý z realizovaných útoků je nebo musí mít příčinu či impuls, aby k němu došlo. Realita se ukázala zcela jiná. Je naprosto liché se domnívat, že pokud budu vlastníkem nebo provozovatelem informačního systému, který není středem zájmu skupiny osob nebo jednotlivce jsem zbaven hrozby v podobě napadení nebo zneužití. Ano, riziko se zmenšuje, nikoliv eliminuje. Čím exponovanější mé systémy budou, tím bude i vyšší riziko jejich napadení nebo zneužití. Pokud budu mít ve své správě relativně exponované systémy, jakým způsobem zajistím, aby k napadení nebo zneužití nedošlo? Odpověď na tuto otázku zní, *velmi špatně* nebo *nemá řešení*. Ze zkušeností je patrné, že i ty nejlépe zabezpečené systémy, které využívají nejnovějších opatření a trendů dané doby jsou napadnutelné a je jen otázka, jak velkou motivací a jakými prostředky útočník disponuje. Vztah mezi impulzem k útoku a samotnou realizací je z časového hlediska zcela irelevantní. Toto mi potvrdil i současný vedoucí týmu vládního CERT (Mgr. Radim Ošťádal).

Z výše uvedeného se může zdát, že vše je marné. Osobně si to nemyslím. Je velmi dobrým počinem přijetí zákona o kybernetické bezpečnosti a zřízení NCKB. Jedná se zatím o nejúčinnější nástroj, jak čelit hrozbám skrytých v kyberprostoru. Pokud by došlo k útokům, které jsem popisoval v rámci operace AntiSec na Českou republiku, dá se předpokládat, že sdílením informací mezi správci ICT veřejné i soukromé správy a přijetím patřičných opatření, by došlo k minimalizaci škod a tím by byla zajištěna ochrana významných i kritických informačních systémů.

12 Závěr

V první části této práce jsem se snažil nastínit problematiku kybernetické bezpečnosti s vymezením pojmů a nastíněním stavu v ČR. V další části jsem se zabýval vybranými hrozbami. Jako modelový případ jsem si vzal hackerské skupiny Anonymous a LulzSec, které se spojily, aby jak samy uvedly, poukázaly na zranitelnost informačních systémů a webových stránek vládních úřadů a firem pod hlavičkou operace AntiSec. Z analýzy jednotlivých útoků provedených různými hackery vyplývá velká rozmanitost důvodů a pohnutek, které k útoku vedly. Má hypotéza, postavená na závislosti času mezi odezvou/útokem na podnět/impulz se nepotvrdila, neboť cílem útoku se stal informační systém s nízkým zabezpečením umožňující útočníkovu penetraci. Ukázalo se také, že hlavním faktorem pro úspěšný útok je motivace a prostředky, kterými útočník disponuje.

Pokud by došlo k podobným útokům na informační systémy, významné informační systémy nebo systémy kritické infrastruktury v České republice, dá se předpokládat, že by část útoků byla úspěšná. To však do chvíle jejich detekce a zavedení opatření. Tato opatření by byla prostřednictvím CERT/CSIRT týmů avizována a distribuována ostatním správcům informačních systémů. Po jejich zavedení by další útok již nebyl úspěšný.

Pokud budou dodržována pravidla, která jsou nastavena současnou legislativou a veškeré složky zapojené do řešení kybernetické bezpečnosti budou kooperovat, účastnit se školení a cvičení, můžeme předpokládat, že počet úspěšných útoků na informační a komunikační systémy bude minimální.

13 Seznam literatury

AFP. 2011. 'Anonymous' hackers access Austrian bank data. *http://phys.org/.* [Online] 25. Červenec 2011. http://phys.org/news/2011-07-anonymous-hackers-access-austrian-bank.html.

ALBANESIUS, CHLOE. 2011. Anonymous 'AntiSec' Operation Targets Viacom, Universal Music. *pcmag.com.* [Online] 30. Červen 2011. http://www.pcmag.com/article2/0,2817,2387893,00.asp.

ALBANESIUS, CHLOE. 2011. LulzBoat Sails On: Anonymous Dumps More Arizona Data. *pcmag.com.* [Online] 29. Červen 2011. http://www.pcmag.com/article2/0,2817,2387817,00.asp.

ARTHUR, CHARLES, GODFREY, HANNAH a QUINN, BEN. 2011. Sun website hacked by LulzSec. *theguardian.com.* [Online] 18. Červenec 2011. http://www.theguardian.com/media/2011/jul/18/sun-website-hacked-lulzsec.

BÍLÝ, Pplk. Miloš. 2012. http://rehabilitovani-vojaci.cz/. *ÚR VSR AČR.* [Online] 13. Leden 2012. http://rehabilitovani-vojaci.cz/files/Ohrozuje-nas-kyberneticka-valka.pdf.

BREWSTER, Tom. 2011. Pfizer's Facebook hacked in AntiSec hit. *itpro.co.uk.* [Online] 22. Červenec 2011. http://www.itpro.co.uk/635131/pfizers-facebook-hacked-in-antisec-hit.

BRIGHT, Peter. 2011. Anonymous vows revenge after 15 arrested; AntiSec hacks continue. *arstechnica.com/.* [Online] 8. Červenec 2011. http://arstechnica.com/security/2011/07/anonymous-vows-revenge-after-15-arrested-in-italy-antisec-hacks-continue/.

ČÍŽEK, Jakub. 2011. Anonymous a LulzSec spouští společnou hackerskou operaci AntiSec. *Živě.cz.* [Online] 21. Červen 2011. http://www.zive.cz/bleskovky/anonymous-a-lulzsec-spousti-spolecnouhackerskou-operaci-antisec/sc-4-a-157581/default.aspx.

GAYATHRI, Amrutha. 2011. Anonymous takes down Tunisian government site in the name of AntiSec; Calls it fight against Internet censorship. *ibtimes.com.* [Online] 28.

Červen 2011. http://www.ibtimes.com/anonymous-takes-down-tunisian-government-site-name-antisec-calls-it-fight-against-internet-294079.

GREENBERG, Andy. 2011. Undeterred By Arrests, Anonymous Spills Data From FBI Contractor ManTech. *forbes.com.* [Online] 30. Červenec 2011. http://www.forbes.com/sites/andygreenberg/2011/07/29/undeterred-by-arrests-anonymous-spills-data-from-fbi-contractor-mantech/.

GROS, Ivan. 2003. *Kvantitativní metody v manažerském rozhodování.* Praha : GRADA, 2003.

CHIRGWIN, Richard. 2011. Operation Antisec lames out again. *theregister.co.uk.* [Online] 4. Červenec 2011. http://www.theregister.co.uk/2011/07/04/when_is_a_leak_not_a_leak.

JIJO, Jacob. 2011. AntiSec Spews Out 53,000 .mil E-mail Addresses After Hack on U.S. Military. *ibtimes.com.* [Online] 13. Červenec 2011. http://www.ibtimes.com/antisec-spews-out-53000-mil-e-mail-addresses-after-hack-us-military-298091.

JIROVSKÝ, V. 2007. *Kybernetická kriminalita.* Praha : Grada Publishing, 2007. stránky 269-274. ISBN 978-80-247-1561-2.

KÁCHA, Pavel. 2009. Adapting the Ticket Request System to the Needs of CSIRT Teams. *WSEAS Transactions on Computers.* 27. 11 2009, stránky 1440-1450. ISSN 1109-2750.

KAZMI, Ayesha. 2011. How Anonymous emerged to Occupy Wall Street. *the Guardian.* [Online] 27. Září 2011. http://www.theguardian.com/commentisfree/cifamerica/2011/sep/27/occupy-wall-street-anonymous.

KUMAR, Mohit. 2011. Anonymous Hacks FBI Contractors IRC Federal. *http://thehackernews.com/.* [Online] 8. Červenec 2011. http://thehackernews.com/2011/07/anonymous-hacks-fbi-contractors-irc.html.

KUMAR, Mohit. 2011. Stevens Institute of Technology hacked; user data dumped. *databreaches.net.* [Online] 8. Červenec 2011. http://www.databreaches.net/stevens-institute-of-technology-hacked-user-data-dumped/.

KUMAR, Mohit. 2011. Thehacker12 Dumps Logins for 20,000 Customers and U.S. Employees. *http://thehackernews.com/.* [Online] 24. Srpen 2011. http://thehackernews.com/2011/08/thehacker12-dumps-logins-for-20000.html.

MAITY, Prarthito. 2011. Flash: Apple hacked; Will iPhone 5 and iPad 3 release dates be affected? *ibtimes.com.* [Online] 4. Červenec 2011. http://www.ibtimes.com/flash-apple-hacked-will-iphone-5-ipad-3-release-dates-be-affected-295797.

MALÝ, Mgr. Jiří. 2012. Důvodová zpráva NCKB. *Národní bezpečnostní úřad.* [Online] 3. Únor 2012. www.nbu.cz/download/nodeid-897/.

MCMILLAN, Robert. 2011. Brazilian Government, Energy Company Latest LulzSec Victims. *PCWorld.* [Online] 22. Červen 2011. http://www.pcworld.com/article/230902/article.html.

MENN, Joseph. 2011. Teen thought to be core hacker. *ft.com.* [Online] 20. Červenec 2011. http://www.ft.com/intl/cms/s/0/d62b179a-b2e9-11e0-86b8-00144feabdc0.html#axzz3Xm5EBdXw.

MILLS, Elinor. 2011. AntiSec hackers post stolen police data as revenge for arrests. *cnet.com.* [Online] 6. Srpen 2011. http://www.cnet.com/news/antisec-hackers-post-stolen-police-data-as-revenge-for-arrests/.

MOOS, Jiří. 2012. CDR. *CDR.* [Online] 17. Duben 2012. http://cdr.cz/clanek/lulzsec-vznik-a-pad-tymova-zrada.

NATO. 2015. The history of cyber attacks - a timeline. *North atlantic treaty organization.* [Online] 9. Březen 2015. http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm.

Návrh vyhlášky, 174/14. 2014. 174/14 Návrh vyhlášky o významných informačních systémech a jejich určujících kritériích; T: 23.10.2014. *Hospodářská komora.* [Online] 23. Říjen 2014. http://www.komora.cz/pro-podnikani/legislativa-a-

normy/pripominkovani-legislativy/nove-materialy-k-pripominkam/174-14-navrh-vyhlasky-o-vyznamnych-informacnich-systemech-a-jejich-urcujicich-kriteriich-t-23-10-2014.aspx.

NBÚ. 2012. Věcný záměr. *Národní bezpečnostní úřad.* [Online] 2012. http://www.nbu.cz/download/nodeid-897/.

NCKB. 2012. Strategie a Akční plán. *Národní centrum kybenetické bezpečnosti.* [Online] 2012. https://www.govcert.cz/download/nodeid-727/.

Novinky. 2015. Téma Novinky. [Online] 7. Duben 2015. http://tema.novinky.cz/anonymous.

OLSONOVÁ, Parmy. 2012. *We Are Anonymous.* Praha : Práh, 2012. ISBN 978-80-7252-400-6.

PAULI, Darren. 2011. Anonymous dumps 2500 accounts, claims Monsanto hack. *itnews.com.au.* [Online] 13. Červenec 2011. http://www.itnews.com.au/News/263556,anonymous-dumps-2500-accounts-claims-monsanto-hack.aspx.

PŘECH, Vladimír. 2014. BOJ S BEZPEČNOSTNÍMI HROZBAMI JE NEPŘETRŽITÝ PROCES. *KYBEZ Portál kybernetické bezpečnosti.* [Online] 30. Červen 2014. https://www.kybez.cz/zpravy/-/blogs/boj-s-bezpecnostnimi-hrozbami-je-nepretrzity-proces.

PŘIBYL, T. 2014. *Kyberšpionáž v proměnách času. Security Word.* 2014.

RAPOZA, Kenneth. 2011. LulzSec Strikes Brazil Again; Petrobras Denies Being Hacked. *Forbes.com.* [Online] 25. Červen 2011. http://www.forbes.com/sites/kenrapoza/2011/06/25/lulzsec-strikes-brazil-again-petrobras-denies-being-hacked/.

READ, Max. 2011. Obama Assassinated, According to Hacked Fox News Twitter. *gawker.com.* [Online] 4. Červenec 2011. http://gawker.com/5817895/hacked-fox-news-tweets-that-obama-is-dead.

REISINGER, Don. 2011. cnet.com. *Anonymous ready to roll in post-LulzSec world.* [Online] 27. Červen 2011. http://www.cnet.com/news/anonymous-ready-to-roll-in-post-lulzsec-world/.

SHAER, Matthew. 2011. Anonymous temporarily brings down Arizona police websites. *csmonitor.com.* [Online] 1. Červenec 2011. http://www.csmonitor.com/Technology/Horizons/2011/0701/Anonymous-temporarily-brings-down-Arizona-police-websites.

SKILLINGS, Jonathan. 2011. AntiSec hackers target Vanguard Defense exec. *cnet.com.* [Online] 19. Srpen 2011. http://www.cnet.com/news/antisec-hackers-target-vanguard-defense-exec/.

STEVENSON, Alastair. 2011. Anonymous Hackers Hit NATO: One Gigabyte of Military Data Lost. *ibtimes.co.uk.* [Online] 21. Červenec 2011. http://www.ibtimes.co.uk/anonymous-hackers-sabu-nato-hack-news-release-data-military-security-antisec-anti-184354.

STEVENSON, Alastair.. 2011. Anonymous Led Hackers Hit Peru, Colombia, Philippines Governments. *ibtimes.co.uk.* [Online] 26. Červenec 2011. http://www.ibtimes.co.uk/anonymous-hackers-hack-government-fbi-italian-hacked-antisec-lulzsec-security-anti-security-operatio-186761.

STEVENSON, Alastair.. 2011. AntiSec hacking Boom: On the anniversary of the Sivas Katliamı Anonymous and allies RedHack deface 1000 websites. *ibtimes.co.uk.* [Online] 5. Červenec 2011. http://www.ibtimes.co.uk/anonymous-redhack-turkey-sivas-katliam-massacre-adnan-oktar-websites-hack-1000-protest-174362.

STEVENSON, Alastar. 2011. AntiSec: Anonymous hackers strike again in "Turkish Takedown Thursday". *ibtimes.co.uk.* [Online] 7. Červenec 2011. http://www.ibtimes.co.uk/antisec-anonymous-hackers-turkey-hack-operation-anti-security-internet-lulzsec-redhack-175785.

ŠENOVSKÝ M., ADAMEC V., ŠENOVSKÝ P. 2007. *Ochrana kritické infrastruktury 1. Vydání.* Ostrava : Edice SPBI Spektrum, 2007. str. 141. 978-80-7385-025-8.

ŠNAJDR, Petr. 2015. Expert: Anonymous útoky projevují nesouhlas, IS ale neohrozí. *aktualne.cz.* [Online] 14. Leden 2015. http://zpravy.aktualne.cz/domaci/ceka-nas-digitalni-valka-ptejte-se-odbornika/r~65dd8e849bd711e49e4b0025900fea04/.

TELEGTAPH, The. 2011. Hackers post documents from Italian cybercrime unit. *telegraph.co.uk.* [Online] 25. Červenec 2011. http://www.telegraph.co.uk/technology/internet/8660683/Hackers-post-documents-from-Italian-cybercrime-unit.html#.

TIMES. 2011. Operation Anti-Security: Anonymous release the identities of 2800 Columbian Black Eagles Special Police Unit members. *INTERNATIONAL BUSINESS TIMES.* [Online] 24. Červen 2011. http://www.ibtimes.co.uk/anonymous-black-eagles-columbia-drug-trafficking-operation-anti-security-lulzsec-hack-hacker-data-da-169177.

TSOTSIS, Alexia. 2011. LulzSec Releases Arizona Law Enforcement Data, Claims Retaliation For Immigration Law. *http://techcrunch.com/.* [Online] 23. Červen 2011. http://techcrunch.com/2011/06/23/lulzsec-releases-arizona-law-enforcement-data-in-retaliation-for-immigration-law/.

WARWICK, Ashford. 2011. Anonymous claims hack of Texas police website despite clampdown by authorities. *computerweekly.com.* [Online] 2. Září 2011. http://www.computerweekly.com/news/2240105492/Anonymous-claims-hack-of-Texas-police-website-despite-clampdown-by-authorities.

WeltN24. 2015. Hacker sind in Deutschland so aktiv wie nie. *DIE WELT.* [Online] 7. Duben 2015. http://www.welt.de/print/welt_kompakt/print_wirtschaft/article116193790/Hacker-sind-in-Deutschland-so-aktiv-wie-nie.html.

WILSON, Drew. 2011. Anonymous Posts Internal Data of the Orange County Democrats. *zeropaid.com.* [Online] 3. Červenec 2011. http://www.zeropaid.com/news/94103/anonymous-posts-internal-data-of-the-orange-county-democrats/.

WILSON, Drew. 2011. P0keu Dumps Usernames and Passwords of TamilCanadian.com to Pastebin. *zeropaid.com.* [Online] 6. Červenec 2011.

http://www.zeropaid.com/news/94214/p0keu-dumps-usernames-and-passwords-of-tamilcanadian-com-to-pastebin/.

14 Seznam zkratek

CERT - Computer Emergency Response Team

CSIRT - Computer Security Incident Response Team

ČR – Česká republika

ČSOB - Československá obchodní banka

DDoS - Distributed Denial of Service

EU – Evropská unie

FBI - Federal Bureau of Investigation

FTP - File Transfer Protocol

GB - Gigabyte

ICT - Information and Communication Technologies

ISAF - International Security Assistance Force

ISMS - Information Security Management System

MB - Megabyte

N/A – Not Available

NASA - National Aeronautics and Space Administration

NATO - North Atlantic Treaty Organization

NBÚ – Národní bezpečnostní úřad

NCKB – Národní centrum kybernetické bezpečnosti

SOCA - Serious Organised Crime Agency

USA - United States of America

15 Seznam tabulek

16 Seznam grafů

17 Přílohy

Přílohy

Salutations Lulz Lizards,

As we're aware, the government and whitehat security terrorists across the world continue to dominate and control our Internet ocean. Sitting pretty on cargo bays full of corrupt booty, they think it's acceptable to condition and enslave all vessels in sight. Our Lulz Lizard battle fleet is now declaring immediate and unremitting war on the freedom-snatching moderators of 2011.

Welcome to Operation Anti-Security (#AntiSec) - we encourage any vessel, large or small, to open fire on any government or agency that crosses their path. We fully endorse the flaunting of the word "AntiSec" on any government website defacement or physical graffiti art. We encourage you to spread the word of AntiSec far and wide, for it will be remembered. To increase efforts, we are now teaming up with the Anonymous collective and all affiliated battleships.

Whether you're sailing with us or against us, whether you hold past grudges or a burning desire to sink our lone ship, we invite you to join the rebellion. Together we can defend ourselves so that our privacy is not overrun by profiteering gluttons. Your hat can be white, gray or black, your skin and race are not important. If you're aware of the corruption, expose it now, in the name of Anti-Security.

Top priority is to steal and leak any classified government information, including email spools and documentation. Prime targets are banks and other high-ranking establishments. If they try to censor our progress, we will obliterate the censor with cannonfire anointed with lizard blood. It's now or never. Come aboard, we're expecting you...

History begins today.

Lulz Security, (ČÍŽEK, 2011)

Friends around the globe,

We are Lulz Security, and this is our final release, as today marks something meaningful to us. 50 days ago, we set sail with our humble ship on an uneasy and brutal ocean: the Internet. The hate machine, the love machine, the machine powered by many machines. We are all part of it, helping it grow, and helping it grow on us.

For the past 50 days we've been disrupting and exposing corporations, governments, often the general population itself, and quite possibly everything in between, just because we could. All to selflessly entertain others - vanity, fame, recognition, all of these things are shadowed by our desire for that which we all love. The raw, uninterrupted, chaotic thrill of entertainment and anarchy. It's what we all crave, even the seemingly lifeless politicians and emotionless, middle-aged self-titled failures. You are not failures. You have not blown away. You can get what you want and you are worth having it, believe in yourself.

While we are responsible for everything that The Lulz Boat is, we are not tied to this identity permanently. Behind this jolly visage of rainbows and top hats, we are people. People with a preference for music, a preference for food; we have varying taste in clothes and television, we are just like you. Even Hitler and Osama Bin Laden had these unique variations and style, and isn't that interesting to know? The mediocre painter turned supervillain liked cats more than we did.

Again, behind the mask, behind the insanity and mayhem, we truly believe in the AntiSec movement. We believe in it so strongly that we brought it back, much to the dismay of those looking for more anarchic lulz. We hope, wish, even beg, that the movement manifests itself into a revolution that can continue on without us. The support we've gathered for it in such a short space of time is truly overwhelming, and not to mention humbling. Please don't stop. Together, united, we can stomp down our common oppressors and imbue ourselves with the power and freedom we deserve.

So with those last thoughts, it's time to say bon voyage. Our planned 50 day cruise has expired, and we must now sail into the distance, leaving behind - we hope - inspiration, fear, denial, happiness, approval, disapproval, mockery, embarrassment, thoughtfulness,

jealousy, hate, even love. If anything, we hope we had a microscopic impact on someone, somewhere. Anywhere.

Thank you for sailing with us. The breeze is fresh and the sun is setting, so now we head for the horizon.

Let it flow...

Lulz Security - our crew of six wishes you a happy 2011, and a shout-out to all of our battlefleet members and supporters across the globe

Zdroj: http://www.businessinsider.com/lulzsec-finished-2011-6#ixzz3ZlNfSaiQ