Česká zemědělská univerzita

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Problematika národních CERTs zemí EU

Bc. Jaroslav Moc

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačních technologií

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Moc Jaroslav

Veřejná správa a regionální rozvoj nav.- Hradec

Název práce

Problematika národních CERTs zemí EU

Anglický název

The issue of national CERTs of EU states

Cíle práce

Hlavním cílem práce je analyzovat okolnosti vzniku národních týmů při ochraně kritické infrastruktury v odvětví informačních a komunikačních systémů v členských státech Evropské unie s jejich napojením na instituty ENISA, CERT-EU a neevropské instituty jako např. CERT, FIRST a jiné. Dále je řešena jejich koordinace, efektivita, účinnost při řešení a předcházení bezpečnostním incidentům a rostoucím kybernetickým hrozbám, včetně prevence a povědomí v oblasti internetu, vyžadující společný přístup s různými CERTs a CSIRTs s podporou národních vlád.

Metodika

Hlavní metodou práce bude komparace a dokumentová analýza, která bude využita především k interpretaci odborných materiálů zpřístupněných zejména prostřednictvím webových stránek jednotlivých národních CERTs a mezinárodních institucí, včetně bezpečnostních opatření pro ochranu kritické infrastruktury vycházející z institutů jako např. Common Criteria, ISO/IEC 27032:2012, nařízení a politik EU nebo NATO. Výstupem práce bude analytická zpráva zaměřená na rozdílnost právního ukotvení, rozsahu pravomocí a působnosti jednotlivých CERTs v prostředí vybraných států.

Harmonogram zpracování

1. Studium odborných informačních zdrojů, stanovení dílčích cílů a postupu řešení: 06/2013
2. Zpracování přehledu řešené problematiky: 07/2013 – 08/2013
3. Vypracování vlastního řešení, diskuse, doporučení a závěry: 09/2013 - 02/2014
4. Tvorba finálního dokumentu práce: 02/2014 – 03/2014
5. Odevzdání práce a tezí: 03/2014

Rozsah textové části

50 - 60 stran

Klíčová slova

CERT, CSIRT, CIRC, ENISA, CERT-EU, Kritická informační struktura, Kybernetická bezpečnost.

Doporučené zdroje informací

1. CCRA. Common Criteria for Information Technology Security Evaluation [on-line]. 321 s. PDF. 2012. Dostupný z WWW: < http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R4.pdf>.
2. CERT-EU. [on-line]. 2013. Dostupný z WWW: <http://cert.europa.eu>.
3. European Commission. Critical Information Infrastructure Protection [on-line]. 2013. Dostupný z WWW: <http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm>.
4. ISO/IEC 27032:2012. Information technology - Security techniques - Guidelines for cybersecurity. 2012.
5. Kümmel, Roman. Cross-Site Scripting v praxi. Zlín: Tigris spol. s r. o. 2011. 332 s. ISBN 978-80-86062-34-1.
6. NATO Cooperative Cyber Defence Centre of Excellence. National Cyber Security Framework Manual [on-line]. 253 s. PDF. 2012. Dostupný z WWW: <http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf>.

Vedoucí práce

Vaněk Jiří, Ing., Ph.D.

Termín odevzdání

březen 2014

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE
Provozně ekonomická fakulta

doc. Ing. Zdeněk Havlíček, CSc.
Vedoucí katedry

prof. Ing. Jan Hron, DrSc., dr. h. c.
Děkan fakulty

V Praze dne 1.11.2013

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Problematika národních CERTs zemí EU" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne ..... _____

Poděkování

Rád bych touto cestou poděkoval vedoucímu práce Ing. Jiřímu Vaňkovi, Ph.D. za příkladné vedení, objektivnost, rady a připomínky v průběhu zpracování.

Problematika národních CERTs zemí EU

The issue of national CERTs of EU states

Souhrn

Diplomová práce je zaměřena na okolnosti vzniku národních týmů při ochraně kritické infrastruktury v odvětví informačních a komunikačních systémů v členských státech Evropské unie s jejich napojením na instituty ENISA, CERT-EU, a neevropské instituty jako např. CERT, FIRST a jiné. Dále je řešena jejich koordinace, efektivita, účinnost při řešení a předcházení bezpečnostním incidentům a rostoucím kybernetickým hrozbám, včetně prevence a povědomí v oblasti internetu, vyžadující společný přístup s různými CERTs a CSIRTs s podporou národních vlád. Výstupem práce je analytická zpráva zaměřená na rozdílnost právního ukotvení, rozsahu pravomocí a působnosti jednotlivých CERTs v prostředí vybraných států.

Klíčová slova: CERT, CSIRT, CIRC, ENISA, CERT-EU, Kritická informační struktura, Kybernetická bezpečnost.

Summary

The thesis is focused on the circumstances of the national teams in the protection of critical infrastructure in the Member States of the European Union, with their links to the institutes ENISA, CERT-EU and non-EU institutions such as CERT, FIRST and others. Furthermore, their coordination, efficiency, effectiveness in addressing and preventing security incidents and increased cyber threats, including prevention and awareness in the Internet, requiring a common approach with different CERTs and CSIRTs with the support of national governments. The result of the work is the analytical report focusing on the diversity of the legal anchoring, scope of powers and authority of CERTs environment in selected states.

Keywords: CERT, CSIRT, CIRC, ENISA, CERT-EU, Critical information structure, Cybersecurity.

OBSAH

1. Úvod

Digitalizace kritických infrastruktur poskytuje značné výhody z hlediska ekonomického vývoje - zlepšení produktivity, lepší konektivitu (propojení), větší efektivitu. Přesto některé z těchto vlastností nesou značná rizika. Každá konektivita do Internetu je svým způsobem předzvěstí nové kybernetické doby, nesoucí vyšší riziko z pohledu narušení a zničení prostřednictvím on-line aktivit. Nová realita představuje kybernetickou špionáž, počítačovou trestnou činnost, a kybernetický terorismus. I přes zdánlivě virtuální povahu těchto hrozeb, jsou fyzické následky velmi hmatatelné.

Internet je dnes prostředkem existence a zdrojem příjmů. Kybernetická bezpečnost se tak stává důležitou součástí internetu samého včetně všech poskytovaných služeb, které nabízí. Znalost kybernetické bezpečnosti se tak stává určitou výhodou, která vede k dynamickému růstu bezpečnostního průmyslu jak ve státním, tak i soukromém sektoru. Firmy mohou exportovat své znalosti prostřednictvím spolupráce mezi oběma sektory. Problematika kybernetické bezpečnosti je již nedílnou součástí každého státu s méně či více vyspělou informační a komunikační technologií. Zvyšuje se nárůst celého spektra trestné činnosti včetně případů kybernetického terorismu prostřednictvím informačních technologií. Bezpečnostní složky států se potýkají s obtížemi v boji proti kybernetickým hrozbám. Stále více finančních prostředků se vynakládá na organizační a technické prostředky, které mají těmto hrozbám zabránit případně zmírnit jejich dopad vně státu. Přístupy jednotlivých států k řešení kybernetické bezpečnosti jsou do značné míry odlišné. V rámci Evropské unie dochází k mezinárodní spolupráci národních týmů vyznačující se společným úsilím při potírání kybernetických hrozeb. Diplomová práce se zaměřuje na okolnosti vzniku zmiňovaných národních týmů při ochraně kritické infrastruktury v odvětví informačních a komunikačních systémů v členských státech Evropské unie s jejich napojením na instituty **ENISA** (European Network and Information Security Agency), **CERT-EU** (Computer Emergency Response Team-European Union), a neevropské instituty jako např. **CERT** (Computer Emergency Response Team), **FIRST** (Forum for Incident Response and Security Teams) a jiné. Dále je řešena jejich koordinace, efektivita, účinnost při řešení a předcházení bezpečnostním

incidentům a rostoucím kybernetickým hrozbám, včetně prevence a povědomí v oblasti internetu, vyžadující společný přístup s různými CERTs a CSIRTs s podporou národních vlád. Bezpečnostní hrozby zůstávají často bez povšimnutí a jsou podceňovány. Minimalizace rizika je závislá i na všech uživatelích přes využití všech dostupných, technických opatření. Nové formy komunikace se staly základem obchodu i zábavy a nelze tak ignorovat nutnost zabezpečení a patřičnou opatrnost.

Termín **CERT** (Computer Emergency Response Team) bude používán v celé práci jako zavedený termín pro bezpečnostní týmy jednotlivých států. Jak bude dále vysvětleno, samotný pojem CERT je registrovaná známka organizace, která jako první reagovala na vznikající problémy počítačové bezpečnosti resp. dnes již zavedený pojem kybernetické bezpečnosti, který bude také dále v práci používán. Jiné definice odlišují týmy na vládní, národní, akademické, komerční, každý nesoucí odpovědnost za daný segment ochrany informační infrastruktury. I u těchto týmů, s výjimkou oficiálních názvů resp. zkratek, bude termín CERT pro účely této práce jednoznačný. Pojmy CERT a později používaný **CSIRT** (Computer Security and Incident Response Team – poskytující širší rozsah služeb), jsou v současnosti používány jako synonymum pro bezpečnostní týmy, i když historicky tomu tak vždy nebylo. Dále existují mezinárodní týmy komerčního, výzkumného a vzdělávacího, neziskového, finančního, nesoucí ve zkratce CERT, CSIRT, a vojenského charakteru **CIRC** (Computer Incident Response Capability) a jiné podoby, o kterých se také zmíníme. Práce je zaměřena na bezpečnostní týmy států Evropské unie, ale nejen z historických, ale i současných událostí je nutné nahlédnout i mimo Evropu. Kybernetický prostor nabízí nové možnosti válečných operací ve virtuálním prostředí, které ovlivňují reálný svět. Anonymní prostředí bez určené geografické vzdálenosti umožňuje útočit komukoliv na kohokoliv. V analytické části práce jsou uvedeny příklady několika posledních let, kdy pojmy kybernetická hrozba, kybernetický útok, kybernetická ochrana, kybernetický prostor mají své pevné místo v reálném čase. Týmy CERT do toho všeho patří a v aktivní spolupráci s jinými subjekty, by měly být nejvyšší autoritou zabezpečující ochranu nás všech.

Na počátku je důležité upozornit, že většina oficiálních institucí vydávající materiály k problematice kybernetické bezpečnosti používá zejména v úvodu svých dokumentů velmi podobná vyjádření v rozsahu slov i vět, která mohou být zavádějící v tom, že daný popis byl použit už někde jinde a je téměř identický. To samé se týká i charakteristiky hlavních cílů jednotlivých bezpečnostních týmů. Porovnáním několika různých dokumentů lze dojít k velmi podobnému textu i v samostatně zpracovávaném novém dokumentu.

Názvy jednotlivých týmů byly převzaty z oficiálních webových stránek. Některé se mohou jevit trochu odlišně, i když jsou součástí jednoho státu a lze tak předpokládat, že minimálně národní doména bude psána stejně, bohužel tomu tak vždy není.

Aktualizace informací bezpečnostních týmů případně jiných subjektů pro obsah této práce skončila ke dni 20.10.2013 s výjimkou aktivit během měsíce října, jako měsíce kybernetické bezpečnosti vyhlášeného v USA, Evropské unii včetně České republiky.

Výstupem práce je analytická zpráva zaměřená na rozdílnost právního ukotvení, rozsahu pravomocí a působnosti jednotlivých CERTs v prostředí vybraných států.

2. Cíl práce a metodika

2.1 Cíl práce

Práce analyzuje problematiku kybernetické bezpečnosti na úrovni národních týmů k ochraně kritické infrastruktury v odvětví informačních a komunikačních systémů členských států Evropské unie a dalších států, které mají výrazný podíl na poli kybernetické bezpečnosti.

Hlavním cílem práce je porovnání působnosti národních týmů zejména členských států Evropské unie.

Dílčími cíli práce jsou:

- vytvoření uceleného přehledu řešené problematiky
- analýza současného stavu ve vybraných evropských státech
- analýza aktuálních hrozeb kybernetické bezpečnosti

Práce je rozdělena na obecnou část, která charakterizuje historické souvislosti vzniku CERTs nejen v zemích Evropské unie, ale i např. v USA, a analytickou část, která je zaměřena na působení jednotlivých týmů členských států Evropské unie, včetně jejich vzájemné spolupráce a spolupráce se soukromým sektorem.

2.2 Metodika

Hlavní metodou práce je komparace a dokumentová analýza, která je využita především ke studiu a analýze odborných zdrojů.

Obecná část nastíní historické souvislosti vzniku CERTs a jejich následný vznik a rozšíření zejména ve státech Evropské unie včetně České republiky.

Analytická část interpretuje odborné materiály jednotlivých národních CERTs a mezinárodních institucí, včetně bezpečnostních opatření pro ochranu kritické infrastruktury vycházející z institutů jako např. Common Criteria, ISO/IEC 27032:2012, nařízení a politik Evropské unie nebo NATO a specializovanými výstupy bezpečnostních firem.

3. Přehled řešené problematiky

Kapitola objasňuje historické souvislosti vzniku CERTs v USA, Asii a Evropě.

3.1 USA a Asie

První pohled patří do USA na **CERT** (není to zkratka, je to jméno a registrovaná ochranná známka Carnegie Mellon University), který byl prvním počítačovým bezpečnostním týmem vůbec, dnes tzv. CSIRT (Computer Security Incident Response Team). Jako první oficiální koordinační centrum, bylo vytvořeno v roce 1988 v reakci na incident tzv. červa Morris (první šíření počítačového viru prostřednictvím internetové sítě, více viz odkaz č. 84), který by v současnosti mohl mít běžný přívlastek kybernetická hrozba. Dnes je CERT důvěryhodná, autoritativní organizace, která se svými projekty zaměřuje na zlepšení bezpečnosti a odolnosti počítačových systémů a sítí. Program CERT je státním majetkem v oblasti kybernetické bezpečnosti, je napojen na Carnegie Mellon University (Software Engineering Institute – federálně financované výzkumné a vývojové centrum). **CERT/CC (**CERT Coordination Center), pravděpodobně nejznámější skupina v rámci Programu CERT, řeší rizika na softwarové a systémové úrovni. I když byl založen jako tým reakce na incidenty, zaměřuje se na identifikaci a řešení stávajících a potenciálních hrozeb, upozornění systémovým administrátorům a dalších technických pracovníků těchto hrozeb a reakce na incidenty různých týmů světa (226) CERT úzce spolupracuje s **US-CERT** (United States Computer Emergency Readiness Team) již od jeho vzniku v roce 1990 (225). US-CERT je součástí the Department of Homeland Security, National Cybersecurity and Communications Integration Center (240) a usiluje o postavení důvěryhodného globálního lídra v oblasti kybernetické bezpečnosti. Mimo jiné koordinuje sdílení kybernetických informací, aktivně řídí kybernetická rizika a chrání ústavní práva amerických občanů. US-CERT využívá programu ochrany kritické informační struktury k zabránění nevhodnému zpřístupnění chráněných informací nebo jiných citlivých údajů (239).

Nezbytnou součástí kybernetické ochrany USA je armádní **USCYBERCOM** (The United States Cyber Command). Oficiálně byl zřízen 21.5.2010, plné operační schopnosti dosáhl 31.10.2010. USCYBERCOM, který je součástí Ministerstva obrany USA, plánuje, koordinuje, integruje, synchronizuje a řídí činnosti přímých operací a obrany stanovených ministerstvem obrany ve všech oblastech kyberprostoru (242).

FIRST (Forum for Incident Response and Security Teams) je uznávaný, globální lídr v reakcích na bezpečnostní incidenty. Členství umožňuje týmům efektivněji reagovat na bezpečnostní počítačové incidenty vládních, vojenských, komerčních a vzdělávacích institucí. FIRST usiluje o podporu spolupráce a koordinace při prevenci incidentů za účelem vyvolání rychlé reakce na mimořádné události podporující sdílení informací mezi členy a společenstvím jako celek. FIRST dále poskytuje služby s přidanou hodnotou např. přístup k aktualizovaným dokumentům obsahující osvědčené postupy, technické semináře s bezpečnostními experty, výroční konference, publikace a webové služby, zájmové skupiny. FIRST má od založení v roce 1990 280 členů z 61 zemí. Byl vytvořen pro lepší spolupráci mezi týmy různých států jako globální fórum týmů vycházející z CERT (133; 134).

APCERT (Asia Pacific Computer Emergency Response Team) usiluje o bezpečný, čistý a spolehlivý kybernetický prostor v pacifickém regionu prostřednictvím globální spolupráce. Udržuje důvěryhodnou kontaktní síť odborníků počítačové bezpečnosti s cílem zlepšit v regionu povědomí a kompetence ve vztahu k incidentům počítačové bezpečnosti (6; 7). Webové odkazy na spolupracující subjekty odkazují na FIRST (Forum of Incident Response and Security Teams), JVN (Japan Vulnerability Notes) a kontaktní bod APCERT (pouze pro členy). Oficiální webové stránky počátek vzniku APCERT neuvádějí, ale podle uvedené, první výroční zprávy (7) z roku 2003 je počátek datován právě do roku 2003. Je zde uváděno 15 zakládajících týmů regionu jako například Austrálie, Čína, Japonsko, Korea, Malajsie, Filipíny, Singapur a další. V roce 2012 je podle výroční zprávy součástí již 30 týmů.

Významným týmem (nejen) asijského regionu je čínský **CNCERT** neboli CNCERT/CC (The National Computer network Emergency Response technical Team/Coordination Center

of China). Čínský CERT je nevládní, neziskovou organizací. Od svého založení v roce 1999 se zaměřuje na předcházení, odhalování, varování a manipulaci čínských síťových bezpečnostních incidentů v souladu s politikou "pozitivní prevence, včasná detekce, rychlá odezva, zaručená obnova", s cílem zajistit bezpečnost veřejného internetu Číny a zajistit bezpečný provoz infrastruktury informačních sítí a životně důležitých informačních systémů. CNCERT je aktivní v rozvoji mezinárodní spolupráce a je otevřený k incidentům zabezpečení sítí na celém světě. Je řádným členem mezinárodní organizace FIRST a jedním z iniciátorů vzniku asijského APCERT. Do roku 2012 vytvořil CNCERT mezinárodní partnerství s 91 organizacemi z 51 zemí nebo regionů. Čína uspořádala první setkání delegátů národních týmů Číny, Koreje (KrCERT/CC – Korea Internet Security Center) a Japonska (JPCERT/CC – Japan Computer Emergency Response Team Coordination Center). Na základě tohoto setkání se potvrzuje posílení spolupráce, která byla započata v roce 2005, s cílem koordinovat kritické incidenty účinnějším a efektivnějším způsobem (60; 61). Příklad spolupráce čínského týmu CERT a společnosti Microsoft viz kapitola 4.3.

3.2 Evropa

CERT-EU (Computer Emergency Response Team-European Union) po tzv. pilotní fázi jednoho roku a úspěšnému vyhodnocení ze strany jiných týmů CERTs, rozhodly orgány EU zřídit stálý CERT-EU k datu 11.09.2012 pro instituce, agentury a orgány Evropské unie. Tým se skládá z IT bezpečnostních odborníků z hlavních institucí Evropské unie (Evropská komise, Generální sekretariát Rady, Evropský parlament, Výbor regionů, Hospodářský a sociální výbor). Je nastavena úzká spolupráce s ostatními týmy CERT v členských státech Evropské unie a specializovanými IT bezpečnostními společnostmi. CERT-EU by měl postupně rozšiřovat své služby, a to na základě požadavků svých nadřízených orgánů s přihlédnutím k dostupným schopnostem, prostředkům a partnerství (27).

Referenční dokument nesoucí označení **RFC 2350** (Request for Comments)[1] specifikuje aktuální osvědčené postupy v celosvětové internetové komunitě týmů CSIRTs. Není možné definovat množinu požadavků, které by byly vhodné pro všechny týmy, ale je možné a užitečné uvést a představit obecný soubor témat a otázek, které jsou předmětem zájmu. Dokument RFC 2350 poskytující základní informace o CERT-EU (29) je zmiňovaný i u dalších týmů.

ENISA CERT. Na domovských stránkách (108) evropské agentury ENISA (European Network and Information Security Agency) je přímý odkaz na ENISA CERT, kde jsou informace o základním poslání každého týmu. Týmy CERTs jsou klíčovými nástroji pro ochranu kritické informační infrastruktury (CIIP - Critical Information Infrastructure Protection). Každý stát využívající služby internetu, musí mít schopnosti pro efektivní a účinné reakce v oblasti informační bezpečnosti. CERTs ale musí udělat mnohem více. Musí působit jako poskytovatelé primární bezpečnostní služby pro vládu a občany. Současně musí jednat jako informační a vzdělávací entita. Ne každá země, která je připojena k internetu,

[1] Historicky první dokument typu RFC-2350 byl publikován v roce 1998 na stránkách IETF (The Internet Engineering Task Force) otevřené komunity síťových inženýrů. Týmy CERT dnes používají dokument jako šablonu pro popis základních požadavků a cílů, více viz http://www.ietf.org/rfc.html.

disponuje kapacitami týmu CERT. Úroveň vyspělosti týmů CERT se dramaticky liší. Posláním agentury **ENISA**, stejně jako jejího týmu CERT je minimalizovat nedostatky tím, že usnadňuje zakládání, školení a cvičení CERTs (101). Na stránkách jsou dále k dispozici základní informace o týmech CERTs, které jsou jedinými institucemi, které mohou řešit nastalé bezpečnostní incidenty. Kromě reaktivních služeb, obvykle poskytují i komplexní portfolio dalších bezpečnostních služeb pro své zákazníky, jako jsou výstrahy a varování, rady a bezpečnostní školení. Během několika let se týmy CIRTs staly primárními poskytovateli bezpečnostních služeb. Za zvýšený zájem o vznik nových týmů jsou zmiňovány zejména kybernetické útoky v Estonsku, dále proti vládám Německa, Švédska a Francie a dalších zemí (více viz kapitola 4). Hranice internetového prostoru neexistují, proto došlo k identifikaci spolupráce jako nutnosti pro úspěšné zvládnutí reakcí na bezpečnostní incidenty. Role agentury ENISA není operativní, ale spíše vystupuje jako prostředník a zprostředkovatel informací pro týmy CERT/CSIRT. Jako odborný orgán musí zůstat v kontaktu se všemi týmy v Evropě i mimo ni. Nadále podporuje vznik subjektů typu CSIRT. Kromě toho bude agentura udržovat a zlepšovat kvalitu svých bezpečnostních služeb, analyzovat funkce, jako je pokročilý výcvik, možné scénáře pro certifikace a odezvy incidentu při cvičení a sestavení osvědčených postupů. ENISA zahájila spolupráci s příslušnými globálními aktéry v oblasti týmů CERT – FIRST, TF-CSIRT (viz dále), US CERT/CC, APCERT, čínským CERT a komunitou ve Spojeném království Velké Británie a Severního Irska. Agentura shromažďuje a šíří osvědčené postupy a publikace (102).

ENISA je ze všech institucí EU nejvýraznější co se odborných výstupů týče (více viz analytická část). Od žádné jiné instituce resp. týmu CERT neexistuje jak v členských zemích EU, mimo ni a jinde ve světě taková produktivita (veřejně přístupná) s informacemi mající vztah ke kybernetické bezpečnosti.

TERENA (Trans-European Research and Education Networking Association) vznikla v roce 1994 sloučením EARN (European Academic and Research Network) a RARE (Réseaux Associés pour la Recherche Européenne). Výzkumná a vzdělávací komunita, jejímž hlavním předmětem činnosti je spolupráce a sdílení znalostí s cílem podpořit rozvoj internetových

technologií, infrastruktury a služeb, které mají být používány v oblasti výzkumu a vzdělávání komunity s protějšky z jiných zemí Evropy. V rámci evropského regionu má TERENA vedoucí postavení umožňující a podporující spolupráci síťových inženýrů a manažerů (215; 216; 217).

TF-CSIRT (The Task Force for Computer Security Incident Response Teams) je pracovní skupinou organizace TERENA podporující spolupráci a koordinaci mezi týmy CSIRT v Evropě a sousedních regionů. TF-CSIRT poskytuje fórum pro členy komunity, kde dochází k výměně zkušeností a znalostí, provozuje systém evidence a akreditace dalších týmů, včetně standardů certifikačních služeb, dále vyvíjí a poskytuje služby pro jiné CERTs, podporuje používání společných norem a postupů pro řešení bezpečnostních incidentů a v případě potřeby koordinuje společné iniciativy (219; 220).

TI - Trusted Introducer (223; 224) původně spadající pod organizaci **TERENA**, od 1.9.2000 oficiálně zahájila v rámci společenství evropských týmů CERT schválenou koncepci služeb poskytované bezpečnostním týmům v Evropě. Trusted Introducer (vycházející z dříve používaného termínu Web of Trust – založeno na osobních vztazích mezi zaměstnanci dotčených týmů, které s rozvojem internetu a nárůstem počtu týmu už není možné) slouží jako středisko pro všechny bezpečnostní týmy – provádí registraci, akreditaci a certifikaci týmů na základě prokazatelných znalostí. Členům umožňuje služby vedoucí ke zlepšení a usnadnění interakce postižených subjektů s tím správným týmem. Poskytuje kompletní adresář kontaktů a dalších užitečných organizací o všech registrovaných, akreditovaných a certifikovaných týmech. Členy TI je pět ze šesti českých týmů (říjen 2013) s tím, že ACTIVE24-CSIRT je ve stavu „listed“ a dva vysokoškolské a dva provozované sdružením CZ-NIC jsou ve stavu „accredited“, vládní GOVCERT.CZ jako člen uveden není, což vyplývá ze statusu danému CZ-NIC (viz kapitola 3.4).

V rámci Evropy dále působí **EGC** (The European Government CERTs group), které je neformálním sdružením evropských vládních týmů CERT**.** Jeho členové účinně spolupracují na základě vzájemné důvěry (již zmiňovaný Web of Trust) a porozumění. Současnými členy

jsou vládní týmy 11 států a to Dánska, Finska, Francie, Nizozemí, Německa, Norska, Spojeného království (dva týmy), Španělska, Švédska, Švýcarska a Rakouska. Proces podávání žádosti o členství je momentálně uzavřen. EGC je funkční skupinou technického zaměření. Neurčuje politiku spadající do kompetence jiných orgánů v rámci jednotlivých států. Členové EGC jednají sami za sebe a na vlastní zodpovědnost. Jednotliví členové participují na činnostech agentury ENISA a přispívají k agenturním výstupům (85; 86).

V roce 2013 byl spuštěn **EC3** (European Cybercrime Centre) jako součást Europolu. EC3 oficiálně zahájil svou činnost k 1. 1. 2013.[2] Zaměřuje se hlavně na kriminalitu spojenou s útoky na online finanční nástroje, sexuální zneužívání dětí a útoky na klíčovou evropskou infrastrukturu. Centrum úzce spolupracuje nejen s Europolem (viz analytická část) a evropskými týmy CERTs, ale také s řadou subjektů z dalších oblastí od mimoevropských států a mezinárodních organizací přes poskytovatele internetových služeb a soukromé společnosti až po akademické a civilní instituce. Zástupci společností (např. Cisco, Fox-IT, Kaspersky, McAfee , Verizon, Trend Micro) jejichž výstupy jsou v analytické části citovány, jsou členy poradní skupiny EC3 pro internetovou bezpečnost (127). Podle vyjádření EC3, přijdou oběti počítačové kriminality ročně na celém světě o 290 miliard USD, což je podle EC3 výnosnější, než celosvětový obchod s drogami (126).

NATO CCD COE (Cooperative Cyber Defence Centre of Excellence) se sídlem v estonském Tallinnu bylo oficiálně založeno dne 14.5.2008 s cílem posílení kybernetické obranyschopnosti NATO. Centrum bylo plně akreditováno v rámci NATO jako mezinárodní vojenská organizace dne 28.10.2008. Projekt "Cyber Security Status Watch" mapuje čtvrtletně aktualizované zvýraznění nedávného mezinárodního vývoje a iniciativy mezinárodních organizací v oblasti kybernetické bezpečnosti. Materiály jsou k dispozici ke stažení na portálu CCD COE. Přístup na Portál je otevřen pro členy NATO a s NATO propojenými osobami,

[2] EC3 má za sebou k 1.1.2014 první rok své existence. Za tu dobu se úspěšně etablovalo jako akceschopná součást boje proti kybernetickým zločincům v rámci Evropské unie, ale i na mezinárodním poli. Zapojilo se třeba do vyšetřování kauz vydírání pomocí ransomwaru, spustilo několik kampaní na boj proti sexuálnímu zneužívání dětí na internetu, více viz http://europa.eu/rapid/press-release_SPEECH-14-114_en.htm?locale=en.
.

úředníky a akademickou obcí zemí NATO a NATO CCD COE partnerskými organizacemi. Vzhledem k rostoucímu počtu subjektů působících v oblasti kybernetické bezpečnosti, může být náročné orientovat se v toku všech těchto právních a politických dokumentů. Cílem projektu "Cyber Security Status Watch" je poskytovat přehled o těchto iniciativách kybernetické bezpečnosti souvisejících s cílem zlepšit celkové povědomí o mezinárodním vývoji a především sloužit jako centrální rozcestník pro snadné přístupy k široké škále různých právních a politických nástrojů, které tvoří současnou doménu kybernetické obrany. Tématy pro druhé čtvrtletí rok 2013 byly: Hlasování Evropského parlamentu pro sankce za kybernetický zločin (viz analytická část); Dosažení konsensu skupiny vládních expertů OSN; Přeshraniční přístup k datům: Quo Vadis, Rada Evropy?; Boj s kybernetickým terorismem; Setkání ministrů obrany zemí NATO na počítačovou ochranu - viz analytická část (16; 17; 22; 23).

Mezi hlavními požadavky NATO bylo vytvoření funkční struktury v oblasti **Cyber Defence/Cyber Security** na národní úrovni, definice národní autority pro oblast Cyber Defence/Cyber Security a vytvoření funkčních kapacit týmů CIRC a struktur CERT/CSIRT. Kybernetický prostor byl definován jako páté bojiště a přiřazen k zemi, moři, vzduchu a vesmíru. Kybernetický útok je roven fyzickému útoku a následné fyzické reakci dotčeného státu. Významnými mezníky bylo zejména zasedání zástupců NATO v Praze v roce 2002, jehož závěrem bylo zahrnutí „Cyber Defence Strategic Concept“ tzv. Strategického konceptu kybernetické obrany do politické agendy. Dále v roce 2004 podpora vzniku armádních týmů CIRC; v roce 2008 na bukurešťském summitu praktická realizace politiky NATO na počítačovou obranu „NATO Cyber Defence Formal Policy & Concept“ a „NATO Cyber Defence Management Authority/Management Board“. Tyto politiky stanoví základní zásady, a stanoví směr NATO s civilními a vojenskými orgány pro zajištění konsolidovaného přístupu ke kybernetické obraně a koordinované reakce na kybernetické útoky. Obsahuje také doporučení jednotlivým spojencům ohledně ochrany národních komunikačních systémů. Politiky jsou podporovány několika vojenskými dokumenty zaměřených na praktické a funkční aspekty kybernetické obrany (74; 124).

V roce 2012 na summitu v Chicagu byla deklarována strategická koncepce „NATO Cyber Defence Full Operational Capability“ která poukazuje na rostoucí propracovanost kybernetických útoků a z toho vyplývající naléhavou ochranu informačních a komunikačních systémů aliance (173).

Je důležité upozornit na výběr odkazů na dokumenty národních politik kybernetické bezpečnosti a to včetně České republiky (21). Jsou zde k dispozici „CYBER SECURITY STRATEGY OF THE CZECH REPUBLIC FOR THE 2011 – 2015 PERIOD“ (104) a **„**Action Plan for Cyber Security Strategy of the Czech Republic for years 2011-2015“ - samotný dokument je pouze v češtině (AKČNÍ PLÁN KE STRATEGII PRO OBLAST KYBERNETICKÉ BEZPEČNOSTI V ČESKÉ REPUBLICE NA OBDOBÍ 2012 – 2015) a přímý odkaz na NBÚ jako národní bezpečnostní autoritu (178). Výše popisované dokumenty jsou k dispozici i na oficiálních stránkách českého vládního CERTu v záložce Legislativa/Další dokumenty (186).

NATO CIRC (Computer Incident Response Capability). Informace nejsou veřejně dostupné. Je nutná registrace garantovaná státním orgánem České republiky (184). Informace o českém CIRC viz kapitola 3.4.

Předchozí týmy jsou nadnárodního charakteru, dále zmíníme týmy národních států evropského regionu – **nizozemský**, z důvodu prvního týmu svého charakteru v Evropě vůbec, a **estonský**, který své aktivity v roce 2007 musel podřídit ruským kybernetickým útokům, kdy došlo k vyřazení národní informační a telekomunikační infrastruktury (viz analytická část). Zhodnocení týmů zemí sousedící s Českou republikou jsou součástí kapitol 3.3 a 4.2.

Nizozemský **GOVCERT.NL** byl zařazen pod **NCSC** (National Cyber Security Center jehož provoz byl zahájen k 1.1.2012). NSCS spolupracuje při posilování obranyschopnosti nizozemské společnosti v digitální doméně. Cílem je dosažení bezpečné, otevřené a stabilní informační bezpečnosti prostřednictvím sdílení znalostí a zkušeností vedoucí k dřívější identifikaci případných hrozeb. Národní síť pro výkon funkce nizozemského týmu mimo jiné

zahrnuje dalších jedenáct státních institucí včetně bezpečnostních složek a komerčního KPN-CERT, jehož historie sahá do roku 1995. Mezi týmy, s kterými NSCS intenzivně spolupracuje, jsou polský NASK resp. CERT Polska (viz následující kapitola), rakouský CERT.au (viz následující kapitola), australský AusCERT, japonský JPCERT, a americké CERT CC a US-CERT (viz předchozí). Spolupráce veřejného a soukromého sektoru je nastavena na tzv. partnerství IRB (the ICT Response Board) kde jsou členy zástupci telekomunikačních společností, dodavatelů energií, bank, vládních orgánů a policie (158; 159; 193; 195; 196; 197).

CERT-NL takto známý do roku 2003, do roku 2007 jako SURFnet-CERT, dnes jako SURFcert, byl založen roku 1992. Působí v oblasti výzkumu a vysokoškolského vzdělávání. Aktivně spolupracuje s dalšími národními a mezinárodními týmy. Vládním a národním týmem je od roku 2002 GOVCERT.NL zařazený od 1.1.2012 v NCSC-NL. V Nizozemí působí (stav k červnu 2013) celkem 14 bezpečnostních týmů z různých oblastí zájmu – vojenské, finanční, akademické a poskytovatelů internetových služeb (111; 210).

CERT-EE (The Computer Emergency Response Team of Estonia) byl založen v roce 2006 jako organizace zodpovědná za řízení bezpečnostních incidentů ve vládních a národních počítačových sítích. Je národním kontaktním místem pro mezinárodní spolupráci v oblasti bezpečnosti informačních technologií. Dokument RFC 2350 dále specifikuje hlavní oblasti působnosti, zejména řešení incidentů počítačové bezpečnosti bez ohledu na příslušnost nebo provozovatele služby, koordinace aktivit v případě rozsáhlejší situace na celostátní úrovni, vzdělává a zvyšuje povědomí uživatelů v oblasti počítačové kriminality, v případě potřeby komentuje situace kybernetického rozsahu, analyzuje, systemizuje a předává informace internetovým poskytovatelům služeb a správcům domén (34; 35; 46; 47).

3.3 Sousední státy – Německo, Polsko, Rakousko, Slovensko

Německý **CERT-Bund** (Computer Emergency Response Team der Bundesverwaltung) je týmem spolkové správy. Má za cíl působit jako ústřední kontaktní místo pro preventivní a reaktivní opatření s ohledem na zabezpečení a dostupnost incidentů v počítačových systémech. IT bezpečnostní incidenty jsou řešeny ve spolupráci se zúčastněnými stranami a CERT-Bund. Základní informace jsou dostupné pouze v němčině (33). Více informací lze získat z dokumentu RFC 2350. Tým je ústředním kontaktním místem v oblasti počítačových bezpečnostních incidentů související s německou vládou, provozuje vnitrostátní národní IT operační a situační centrum (Germany's national IT Situation Centre). Tým je součástí BSI (Bundesamt für Sicherheit in der Informationstechnik - Federal Office for Information Security – Federální úřad pro informační bezpečnost) s gescí německého Ministerstva vnitra (BMI – Bundesministerium des Innern - Federal Ministry of the Interior). CERT-Bund mimo jiné vytváří situační zprávy a poskytuje vzdělání a školení pro vládu. Tým je součástí „Deutscher CERT-Verbund Übersicht“ (Aliance týmů CERT německého veřejného sektoru.) kde je celkem 18 týmů a každý je odpovědný za svou cílovou autonomní skupinu. Německo má vůbec nejvyšší počet (k červnu 2013 jich je 22) bezpečnostních týmů určených k ochraně národních sítí informačních technologií nejen v rámci Evropy, ale i celého světa (32; 36).

Dalším německým týmem je **Bürger-CERT** - projekt BSI. Bürger-CERT upozorňuje a informuje občany a malé podniky na internetové hrozby, dále analyzuje a vyhodnocuje (v hodinových intervalech) bezpečnostní situaci na internetu a přijímá konkrétní opatření (výstrahami) bezpečnosti internetu a e-mailů. Činnost týmu byla zahájena v roce 2006 jako společný projekt BSI a německé společnosti pro IT bezpečnost Mcert. Od června 2007 jsou služby Bürger-CERT poskytovány výhradně BSI, který přijímá odpovědnost za vnitřní IT bezpečnost v Německu. Cílem je dostupné zvyšování povědomí speciálně pro občany využívající internetových služeb (14).

CERT Polska – polský bezpečnostní tým má webové stránky pouze v polštině. Volba angličtiny sice existuje (výjimečně), ale stejně jako jiné informace o samotném týmu jsou pouze v polštině. Na posledním řádku stránky je nevýrazným písmem informace o copyrightu **NASK**. Tím se dostaneme (nejdříve vyhledáním informací o NASK) na web NASK (Research and Academic Computer Network – Výzkumná a akademická síť) připojenou na internet v roce 1991. NASK získal v roce 1993 statut výzkumné a vývojové organizace. Dnes je předním polským operátorem datových sítí. V rámci vědeckých a výzkumných aktivit spolupracuje s Fakultou elektroniky a informačních technologií ve Varšavě, je členem mezinárodních organizací a sdružení (FIRST, CENTR, TERENA, RIPE) a účastní se projektů Evropské unie. Součástí organizace NASK je CERT Polska (odkaz na web bohužel zobrazuje Not Found - nenalezen), úzce spolupracující s dalšími bezpečnostními týmy po celém světě. NASK je polským národním registrátorem internetových jmen v doméně .pl (48; 49; 171).

Rakouský **CERT.at** je rakouským národním CERT. Je primárním kontaktním místem pro informační bezpečnost v národním kontextu. Koordinuje další týmy působící v oblasti kritické a komunikační infrastruktury. Poskytuje základní informace o zabezpečení informačních technologií (výstrahy, varování, rady). V případě významných online útoků namířených proti rakouské infrastruktuře koordinuje reakci cílových subjektů a místních bezpečnostních týmů (40; 41).

Druhý rakouský tým **GovCERT.AT** (the Austrian Government Computer Emergency Response Team) má svůj rozsah v rakouské veřejné správě a kritické informační infrastruktury. Byl založen v dubnu 2008 a jako organizace spadá pod spolkového kancléře. Ve spolupráci s týmem CERT.at preventivně zabraňuje relevantním bezpečnostním incidentům v oblasti informačních a komunikačních technologií (136). První zpráva o činnostech týmů CERT je z roku 2010 (37). K dispozici (přístupné pouze na německé verzi webu) jsou i informace k plnění vnitrostátních úkolů a povinností obou týmů v národním kontextu pro mezinárodní spolupráci (137) a jiných dokumentů (opět pouze v německé verzi) v záložce „Links und Dokumente“ (138).

V rámci důvěry a ochrany sítí elektronické komunikace ve veřejném a soukromé sektoru působí tzv. **CIRCA** (Computer Incident Response Coordination Austria) rakouská celostátní bezpečnostní síť včasného varování před hrozbami ohrožující infrastrukturu. Soukromý sektor je pod kontrolou ISPA (Internet Service Providers Austria) zatímco veřejný sektor pod BKA (Bundeskanzleramt und Krisenmanagement), (39).

Slovenský **CSIRT.SK** byl zřízený Ministerstvem financí Slovenské republiky s cílem zabezpečit přiměřenou úroveň ochrany národní informační a komunikační infrastruktury (72). Dokument RFC 2350 vymezuje CSIRT.SK jako vládní a národní CSIRT, který byl založen jako nezávislé oddělení DataCentrum (rozpočtová organizace v rámci Ministerstva financí Slovenské republiky). Zřízení týmu navrhla slovenská vláda v červenci 2009 v souladu s Národní strategií informační bezpečnosti. Posláním týmu je zvýšení ochrany kritické národní informační infrastruktury, zvyšování povědomí v oblasti bezpečnosti informací a spolupráce s mezinárodními partnery a organizacemi v této oblasti (71). Historické souvislosti vzniku slovenského bezpečnostního týmu viz dokument z dubna 2010 (70).

3.4 Česká republika

Situace v rámci České republiky se zdá být na první pohled poněkud nepřehledná. Vycházíme-li z dokumentu agentury ENISA (103) zveřejněný v červnu 2013 nebo z odkazů českého vládního týmu jsou v České republice: vládní CERT, národní CSIRT, vysokoškolské CESNET-CERT a CSIRT-MU, ACTIVE24-CSIRT a CZ.NIC-CSIRT. U všech týmů je uvedeno, že nejsou členy celosvětového FIRST (interaktivní mapa států je u České republiky neaktivní, oproti všem sousedícím zemím České republiky – stav k červnu 2013).

Vládní CERT (GovCERT) spadající pod **NCKB** (Národní centrum kybernetické bezpečnosti) vznikl na základě usnesení vlády České republiky dne 19.10.2011 se sídlem v Brně. Je součástí Národního bezpečnostního úřadu (NBÚ) jako gestora problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast. Citace z webu: „Úlohou centra je koordinace spolupráce na národní i mezinárodní úrovni při předcházení kybernetickým útokům i při návrhu a přijímání opatření při řešení incidentů i proti probíhajícím útokům.“ Rok 2015 bude pro vládní tým zlomový – Kybernetický zákon (viz analytická část) by měl nabýt účinnosti a Národní centrum kybernetické bezpečnosti má být plně funkční (185).

Národní CSIRT vznikl v roce 2007. Je provozován sdružením **CZ.NIC** (správcem české národní domény – zájmové sdružení právnických osob) a na základě Memoranda uzavřeného v březnu 2012 s NBÚ byl národní CSIRT autoritou budující a rozvíjející agendu, řešící incidenty týkající se kybernetické bezpečnosti v sítích provozovaných v České republice. Plnil i roli PoC (Point of Contact) pro oblast informačních technologií, centra vzdělávání a šíření osvěty v oblasti kybernetické bezpečnosti do doby zřízení vládního CERTu. NBÚ byl koordinátorem mezi národním CSIRT a vládním CERT. Na základě tohoto Memoranda pozbyla po dohodě obou smluvních stran jeho platnost ke dni 31.12.2012. Nové Memorandum nabylo účinnosti dne 1.1.2013 a pozbývá platnosti 31.12.2015 (66; 67; 190).

Dokument **RFC 2350** českého národního týmu uvedený v anglickém jazyce „CSIRT description for CSIRT.CZ, National CSIRT of The Czech Republic“ viz odkaz (62).

CESNET-CERTS je oficiálním názvem bezpečnostního týmu sdružení CESNET (Czech Education and Scientic Network) od ledna 2004. Sdružení CESNET bylo založeno v roce 1996 vysokými školami a Akademií věd České republiky. Rozsah působnosti týmu CESNET-CERTS je pro vysokorychlostní počítačovou síť zvanou CESNET2 propojující největší univerzitní města České republiky a dalších oblastí (57; 58; 59).

Dalším univerzitním bezpečnostním týmem je **CSIRT-MU** (Computer Security Incident Response Team of Masaryk University). Vznikl v květnu 2009 na Ústavu výpočetní techniky Masarykovy univerzity v Brně a byl prvním univerzitním bezpečnostním týmem ze zemí Visegrádské čtyřky. Zabývá se nejen řešením bezpečnostních incidentů, ale také detekcí těchto incidentů v univerzitní počítačové síti včetně osvěty uživatelů v oblasti počítačové bezpečnosti (165; 166).

ACTIVE24-CSIRT je zodpovědný za řešení incidentů a mimořádných událostí v souvislosti s doménami, kde je registrátorem společnost ACTIVE 24, s.r.o., tzn., že působí v komerčním prostředí (1). Společnost se prezentuje jako celoevropsky nejvýznamnější poskytovatel v oblasti hostingu a domén. Historicky byla společnost založena v Oslu v roce 1998, poté následoval vstup na evropské trhy (Nizozemí, Švédsko, Velká Británie a další). V rámci České republiky vložila kapitál do společnosti Globe Internet v roce 2004, kdy došlo i k přejmenování na ACTIVE 24, s.r.o. Datum založení bezpečnostního týmu nelze dohledat ani na webu společnosti, ani CSIRTu, ani na stránkách agentury ENISA, kde je uvedeno šest týmu z České republiky, tak tento jediný nemá uveden datum vzniku (2).

Brněnský **CIRC** (Computer Incident Response Capability) Ministerstva obrany ČR (56) je názorným příkladem, jak by to mělo fungovat. Spravují armádní síť České republiky, ale ve skutečném provozu mají odzkoušeno to, o čem se dlouho mluvilo a stále mluví. CIRC je úspěšný i v rámci kybernetických cvičení NATO např. v roce 2010 se stali pomyslnými vítězi v rámci praktického cvičení „Cyber Coalition 2010“. Informace armádního CIRC jsou veřejně nedostupné. Veškeré zde popsané skutečnosti jsou po osobní návštěvě pracovního charakteru a konzultaci s velitelem a některými členy týmu a autora této práce uskutečněné

v roce 2010. Jedním ze současných členů ENISA CERT je i Andrea Dufková[3], která je podle dostupných údajů bývalou příslušnicí českého armádního týmu CIRC (99).

Česká pobočka **AFCEA** (Armed Forces Communications & Electronics Association) byla založena v květnu 1993. Své aktivity zaměřuje do oblasti podpory a rozvoje informačních a komunikačních technologií ozbrojených sil. Posláním této neziskové a vzdělávací organizace je vytváření profesionálního fóra mezi zástupci silových resortů, státní správy a akademické obce. Česká pobočka je součástí organizace AFCEA International založené v roce 1946 v USA. V současnosti sdružuje více jak 35 tisíc individuálních a více než dva tisíce členů ve více než 130 pobočkách po celém světě (3; 4).

V seznamu týmů na webu CSIRT (51) český národní tým uvedený není. Na svých stránkách přitom uvádí jako jeden ze svých cílů: „Udržování zahraničních vztahů – se světovou komunitou CERT/CSIRT týmů a organizacemi, které tuto komunitu podporují“ (54). Určitě by bylo vhodné, zastupuje-li český národní tým, uvést několik týmů, s kterými spolupracuje, případně spolupracoval v rámci některých aktivit. Ve výroční zprávě za rok 2012 (viz dále) je sice uvedeno několik příkladů spolupráce, ale je to jen jakýsi krátký souhrn. Týmy sousedních států německý, polský a slovenský v seznamu jsou. To samé na webu organizace FIRST (52; 53).

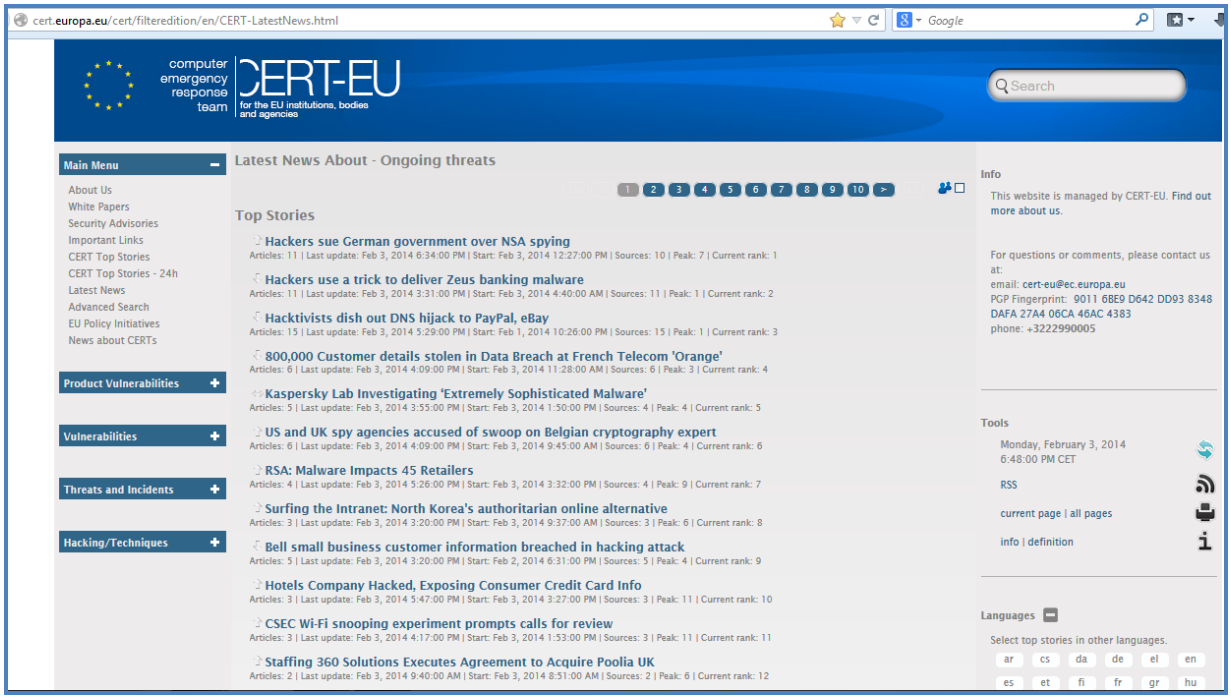
[3] Andrea Dufková je v materiálu agentury ENISA „CERT community“ prezentovaný v listopadu 2013 uvedena jako „main editor“. Dostupné na: http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/cert-community-recognition-mechanisms-and-schemes.

4. Analytická část

Kapitola je zaměřena na konkrétní výstupy jednotlivých CERTs, případně jiných subjektů a eventuálních rozdílností daných výstupů.

4.1 CERT-EU, ENISA

Domovská stránka **CERT-EU** používaná při oficiálním spuštění (28) byla v průběhu roku 2013 změněna na jinou webovou adresu (31) a v současnosti (říjen 2013) je přesměrována i po jejím použití či vepsání ze zkrácené volby (28) je nabízena i v internetových vyhledávačích, a kterou by uživatel s uživatelskou znalostí psaní domovských internetových adres organizací, společností a jiných snad i předpokládal, prostě nefunguje. Úvodní, dnes již domovská stránka (viz Obrázek č. 1) nabízí „Latest News About – Ongoing Threats“ tj. novinky a aktuální hrozby.



Obrázek č. 1: Domovská stránka CERT-EU.
Dostupné na: http://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html (31).

CERT-EU využíval v počátku svého spuštění zejména aktuální zprávy z webu CSIRT s odkazy na články s kybernetickou bezpečností resp. hrozbami, útoky, atd., v současnosti jsou zprávy obsahově poněkud odlišné, ale stále svým obsahem blízké CSIRT. Takzvané „Top Stories“ nejsou ničím jiným než jedním titulkem zprávy označený článek, na který jsou navázány další články se stejným nebo podobným titulkem resp. obsahem. Nutno podotknout, že některé ne-li většina je identickou kopií prvně zveřejněného článku bez jakékoliv přidané hodnoty. To samé je i v oddílech „Articles published more than ...“, kde jsou články publikované před několika minutami, hodinami případně dny – opět bez jakékoliv přidané hodnoty. Tzv. Security White Papers obsahuje posledně zveřejněný dokument k datu 5.11.2012 nazvaný „Incident Response – Data Acquisition Guidelines for Investigation Purposes“. Aktuálnější zprávy k datu 30. října 2013 zde nejsou (30).

Další záložka **Security Advisories** zveřejňuje v jednoduchých (RTF – Reach Text Format) souborech základní informace zmiňovaných bezpečnostních aktualizací společností zejména Microsoft, Oracle, Adobe, Cisco a jiné. **Important Links** – záložka, v které mají být informace pro IT odborníky a manažery. Poslední link/odkaz je z 12.6.2013 na stránky spol. Microsoft na dokument „Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques“ zabývající se útoky proti operačním systémům Windows včetně doporučení snižující závažnost rizika pro útokům typu PTH (Pass-the-Hash) , druhý odkaz je na dokument z 13.3.2013 nazvaný „Critical Controls for Effective Cyber Defense“, zpracovaný konsorciem CCA (the Consortium for Cybersecurity Action), obsahující případové studie s technickými opatřeními a doporučeními pro organizace. Bohužel, další tři záložky mění pouze volbu případně vyhledávání (Search) zpráv podle času. Nejzajímavější záložka **EU Policy Initiatives** nabízí odkazy na kybernetickou strategii (zveřejněnou 7.2.2013) nazvanou „An Open, Safe and Secure Cyberspace“ reprezentující komplexní představu o tom, jak nejlépe předcházet a reagovat na kybernetické útoky a narušení. Strategie mimo jiné podporuje evropské hodnoty svobody a demokracie, a ujišťuje, že digitální ekonomika může bezpečně růst. Konkrétní činnosti jsou zaměřeny na zvyšování počítačové odolnosti informačních systémů, snížení počítačové trestné činnosti a posílení schopnosti EU mezinárodní kybernetickou politikou a počítačové obrany (121).

Dokumenty související s kybernetickou strategií jsou dostupné na webu Evropské komise (120). Další neméně zajímavé odkazy jsou na dokumenty:

„A strategy for a Secure Information Society - Dialogue, partnership and empowerment“ (25).

„EU initiative on Critical Information Infrastructure Protection (CIIP)“ (118).

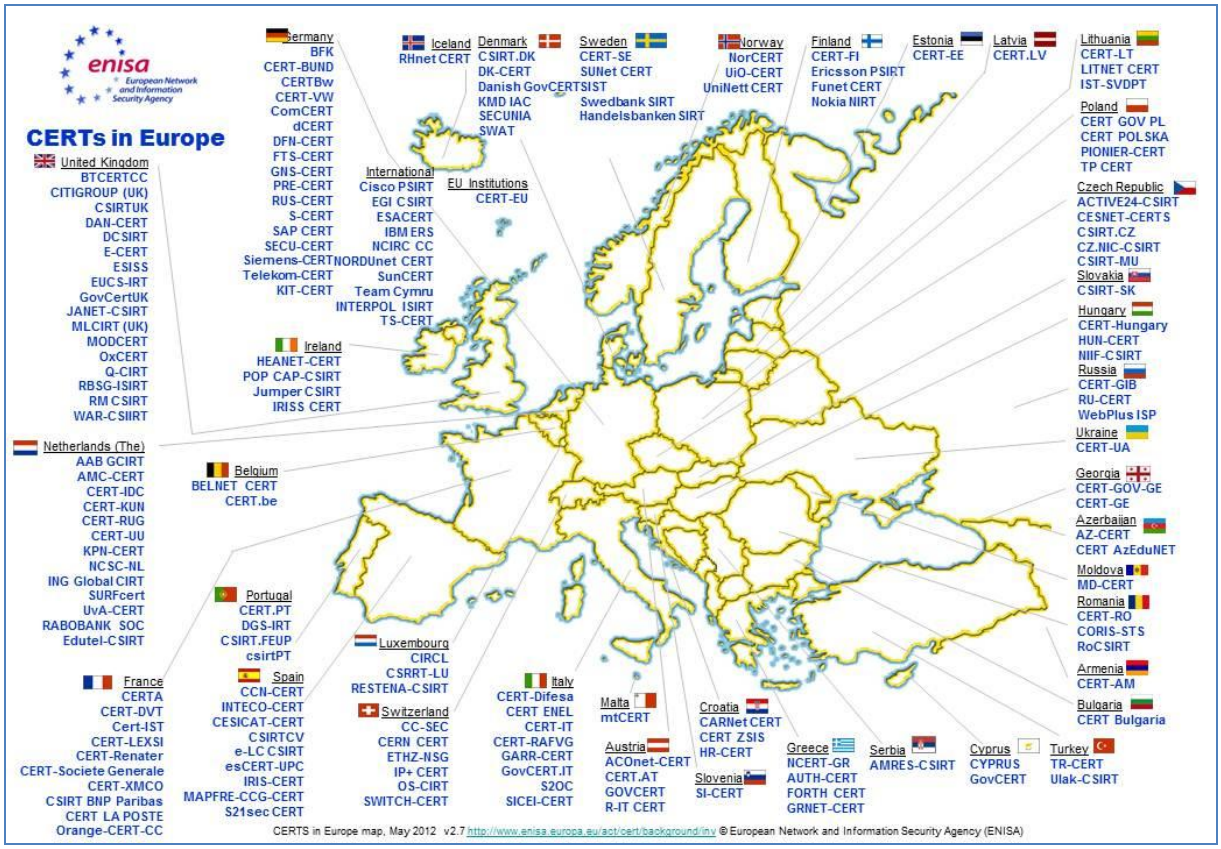
„Digital Agenda for Europe - Pillar III: Trust and Security“ (119).

„The role of the European Network and Information Security Agency (ENISA)“ (108).

Zbylé čtyři záložky opět odkazují na různě členěné články zranitelností, společností, hrozeb a incidentů a hackerskými technikami. Kdo sem zabloudí náhodně nebo velmi zřídka, určitě nebude mít problém s přínosem informací zde získaných, ale pro člověka hledajícího větší množství informací a svým způsobem znalý problematiky kybernetické bezpečnosti, tak stránky **CERT-EU** vyhledávány resp. používány nebudou. Určitě je z tohoto pohledu zajímavější evropská ENISA případně CSIRT. Na stránkách CERT-EU by určitě byl přínosný jakýsi **rozcestník** na jednotlivé CERTs členských států EU včetně jiných evropských a mimo mimoevropských týmů. Bohužel i to zde chybí – je to na stránkách ENISA CERT.

ENISA je v několika posledních letech velmi aktivní (oproti období let 2007 a 2008 kdy nebyly k dispozici žádné výstupy, agentura jakoby existovala pouze formálně a hledala směr, kterým se vydat). Za několik předchozích měsíců (počínaje koncem roku 2012 a následně celý rok 2013) vydala studie jako například „National Cyber Security Strategies. Practical Guide on Development and Execution“, vydáno v prosinci 2012 jako příručka zabývající se národními strategiemi pro oblast kybernetické bezpečnosti. Příručka definuje relevantní oblasti kybernetické bezpečnosti, mapuje evropskou legislativu zabývající se kybernetickou bezpečností a především nabízí užitečné rady jak tvořit, uplatňovat, kontrolovat a upravovat národní strategie kybernetické bezpečnosti jednotlivých členských zemí EU. Za tímto účelem rozlišuje a objasňuje 20 fází tvorby takové strategie (113) dále

"Deployment of Baseline Capabilities of National/Governmental CERTs", dokument vydaný v prosinci 2012 (96) analyzuje situaci národních a vládních CERTs v Evropě s ohledem na jejich schopnosti a nasazení, dále poukazuje na rozdílný přístup výměny informací mezi partnerskými týmy a rozdílnou technickou vyspělostí, mimo jiné i na nedostatečné stanovení rolí a odpovědností, nedostatek finančních prostředků. Novější dokument „Inventory of CERT activities in Europe" (112) vydaný v červnu 2013 poskytuje přehled o aktuální situaci CERTs v Evropě, poskytuje seznam národních týmů včetně podpory a standardizace činností, které se jich týkají. Zmiňovaný dokument obsahuje mapu evropských týmů (viz Obrázek č. 2) včetně interaktivní mapy podle výběru jednotlivých států a typu týmu podle odvětví jako např. vysokoškolské, vojenské, národní, vládní atd.



Obrázek č. 2: „CERTs in Europe" vydaný agenturou ENISA. Dostupné na: http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe (111).

Další v březnu 2013 vydaný tzv. „Flash Note: Cyber-attacks – a new edge for old weapons“ (110) vyzývá nadnárodní společnosti a vládní organizace k urychlenému přijetí opatření pro boj s rozvíjejícími se novými trendy kybernetických útoků.

Přínosem těchto studií je skutečnost, že jsou zde zapracovány **politiky Evropské unie.** Nutno podotknout, že jak stránky ENISA CERT tak i NATO CIRC využívají zpracované informace z webových stránek CERT.org (původní, zastřešující organizaci na univerzitě Carnegie Mellon University's Software Engineering Institute – viz kapitola 3.1).

Agentura **ENISA** zorganizovala druhý ročník mezinárodní konference "2nd ENISA International Conference on Cyber Crisis Cooperation and Exercises" (115), která se konala v Athénách ve dnech 23.-24.9.2013 za účasti více jak 120 manažerů s rozhodovací pravomocí v oblasti kybernetické bezpečnosti z více jak 30 veřejných a soukromých institucí. Konference je platformou určenou pro diskuzi o klíčových trendech a vývoji kybernetických cvičení a spolupráce různých odvětví ve vztahu k internetovým hrozbám, ochraně a kybernetické trestné činnosti. Konference představuje významnou část probíhajícího společného úsilí Evropské unie ke zvýšení bezpečnosti sítí a informací a krizové spolupráce v rámci Evropy i mimo ni. Předchozí první ročník konference „First International Conference Cyber Crisis Cooperation: Cyber Exercises“ se uskutečnil v červnu 2012 v Paříži (94).

„Threat Landscape, Mid-year 2013“ je pololetní zprávou agentury **ENISA** ze září 2013 shrnující např. původce kybernetických útoků stále častěji používající anonymizační (uchovávající soukromí) a decentralizované služby, jako jsou např. sítě P2P (Peer-to-Peer). Podle zprávy lze také předpokládat, že všechny hrozby známé z tradičních oblastí IT se prosadí i na poli mobilních zařízení a hlavním vektorem útoků budou sociální sítě. Malware je navíc stále častěji prodáván jako služba, takže se pravděpodobně zvýší počet různých kampaní. Kybernetické útoky jsou šestým nejčastějším důvodem výpadků komunikačních sítí a následky útoků jsou stále závažnější (105).

Zpráva publikovaná dne 20.8.2013 „Annual Incident Reports 2012“ poskytuje přehled procesů a souhrnných analýz 79 zpráv (z 18 zemí) o nehodách s těžkými výpadky elektronických komunikačních sítí nebo služeb, které byly hlášeny u vnitrostátních regulačních orgánů v průběhu roku 2012. Incidenty uvedené jako hlavní příčiny selhání třetích stran, především selhání napájení, postihly v průměru kolem 2,8 milionu uživatelských připojení. Incidenty zahrnující detailnější způsob přetížení, postihly v průměru kolem 9,4 milionu uživatelských přípojek (100).

Materiál z června 2013 (aktualizované a rozsáhlejší zpracování) „Inventory of CERT activities in Europe“ poskytuje seznam zásahových skupin a podobných zařízení podle zemí, ale také obsahuje katalog spolupráce, podpory a standardizace činností, které se jich týkají (111). K dispozici je i interaktivní mapa týmů CERT podle členských států EU a EFTA. Za Českou republiku jsou zde uvedeny vládní GOVCERT, vysokoškolské CESNET-CERT a CSIRT-MU, národní CSIRT, ACTIVE24-CSIRT a CZ.NIC-CSIRT. U všech týmů je uvedeno, že **nejsou** členy celosvětového **FIRST** (103).

Předchozí zpracování přehledu týmů CERT včetně mapy s názvy týmů jednotlivých států Evropské unie pochází z dubna 2008 (88).

V říjnu 2012 proběhlo simulované kybernetické cvičení **Cyber Europe 2012** kterého se zúčastnilo více než 500 odborníků na kybernetickou bezpečnost, a které prověřilo spolupráci a komunikaci mezi jednotlivými státy a také mezi zainteresovanými subjekty. Cvičení přineslo řadu cenných poznatků. Příští cvičení by se mělo zaměřit více na komunikaci mezi jednotlivými sektory a na konkrétní komunity. ENISA bude nadále zvyšovat informovanost zainteresovaných stran o doporučených postupech a pomocí konferencí podporovat integritu celé komunity. Cvičení potvrdilo přínos zapojení soukromých subjektů a také odhalilo nutnost zapojení dalších sektorů (např. zdravotnictví nebo dopravy) pro větší efektivitu zvládání krizí velkého rozsahu (91; 92).

Předchozí, první cvičení **Cyber Europe 2010** proběhlo v listopadu 2010 (45; 89).

Studie ‚Proactive Detection of Security Incidents“ (publikovaná v listopadu 2012) se zabývá proaktivní obranou proti kybernetickým hrozbám pomocí takzvaných „honeypots“, tj. aplikací monitorujících neoprávněné využívání systémových prostředků, které dovedou zachytit malware a podrobit jej zkoumání. Ve studii bylo zkoumáno celkem 30 těchto open-source nástrojů. Jednotlivé nástroje byly ohodnoceny a byly u nich identifikovány hlavní výhody a nevýhody, na jejichž základě pak byla poskytnuta doporučení jednotlivým skupinám CERT. Mezi nejlépe využitelné řadí ENISA nástroje Dionaea, Glastopf, Kippo a Honeyd. Ostatní mají buď omezené využití, nebo by bylo potřeba investovat prostředky do jejich dalšího vývoje. Podle studie může být aplikace těchto nástrojů velmi účinným prvkem zabezpečení důležitých systémů (95).

ENISA ve zprávě „Cyber Incident Reporting in the EU“ (publikovaná v září 2012) shrnuje všechny články v legislativě Evropské unie, které se týkají kybernetické bezpečnosti. Poukazuje na nedostatky ve stávající legislativě a zdůrazňuje význam legislativních opatření jako základu pro fungující integrovaný systém výměny informací mezi veřejným a soukromým sektorem, hlášení kybernetických incidentů a jejich řešení. Zpráva také popisuje, jak by měl takový systém teoreticky fungovat (93).

Agentura **ENISA** pořádá od roku 2005 semináře pro národní a vládní CERTs členských států Evropské unie. Tematicky jsou semináře zaměřeny od vytváření týmu CERT až po odborná témata aktuálních událostí. V říjnu 2011 se konal v Praze 6th Annual CERT workshop (90) nazvaný „Addressing NIS aspects of cybercrime“ zaměřený na řešení NIS (Network and Information Security) aspektů kybernetické kriminality. Zatím poslední „8th workshop part I“ (97) se konal v květnu 2013 v Bukurešti zaměřený na praktické technické školení národních a vládních týmů CERT. Další plánovaný „8th workshop part II“ (98) se koná v Haagu (Nizozemí) ve spolupráci s EC3 (125) zaměřený na automatizované sdílení informací mezi týmy CERT a vyšetřovacími orgány. Účastníky budou i zástupci **APWG** (The Anti-Phishing Working Group) neziskové, nadnárodní sdružení zaměřující se na odstranění podvodů, zločinů a krádeží identit vyplývající z různých typů kriminální činnosti (9).

Posledním, zde v práci použitým materiálem, je zpráva agentury **ENISA** „National-level Risk Assessments“ zpracovaná v listopadu 2013 zabývající se národními systémy vyhodnocování kybernetických rizik, ve které členským zemím EU doporučuje zlepšit orientaci v problematice kybernetických hrozeb a jejich dopadů, integrovat jednotlivé složky vyhodnocování rizik, podpořit výměnu informací mezi státními a soukromými subjekty a vypracovat podrobný plán pro vyhodnocování kybernetických rizik. V rámci celé Evropské unie by pak měl být vytvořen katalog různých scénářů, měla by být založena trvalá odborná platforma pro výměnu informací a analýza kybernetických rizik by měla být integrována s ostatními mezistátními systémy vyhodnocování rizik (114).

Následující studie a analýzy nadnárodních institucí a společností byly zpracovány z důvodu jejich určité **výjimečnosti a výstižnosti** pro zpracovávanou problematiku.

Internet může být svým způsobem definován jako válečná zóna. Eugen Kasperky (zakladatel spol. Kaspersky Lab a jeden z předních světových odborníků na bezpečnost IT) se zaobírá definicí **kybernetické války** – vedená proti infrastruktuře a ekonomice státu jiným státem a **kybernetického zločinu** – útok vedený proti jednotlivé firmě nebo jednotlivci za účelem obohacení. Rozebírá možnosti plného rozvinutí kybernetické války a uvádí příklady možných útoků vedených v budoucnosti. Zároveň definuje největší problémy s kybernetickými útoky jako např. nedostatečná a pozdní detekce, nízká připravenost. Podle něj se internet stal válečnou zónou, kde informace jsou hlavní kořistí. A navrhuje založení mezinárodního internetového policejního orgánu jako jednoho ze způsobů obrany (150; 227).

Na předchozí věty navazuje prohlášení šéfa **Interpolu** (Ronald K. Noble), že se bude snažit vytvořit celosvětový systém, který by usnadnil boj proti kybernetické kriminalitě. Kybernetičtí zločinci operují napříč státy, a pokud má být jejich stíhání efektivní, je třeba zapojit všechny zainteresované subjekty a sjednotit postupy a právní nástroje. Interpol nyní spolupracuje s bezpečnostní společností Kaspersky Labs, která je ochotná poskytnout svoji expertízu v oblasti kybernetických hrozeb. Právě spolupráce národních orgánů a soukromých společností pak má zajistit větší bezpečnost kyberprostoru (143).

Šéf Interpolu Ronald K. Noble se v březnu 2013 sešel s Eugenem Kasperskym. Jednal s ním o možné spolupráci při potírání kybernetického zločinu. Kaspersky iniciativu ocenil, přislíbil spolupráci a také prohlásil, že podpoří globální výzkumné a vývojové centrum **IGCI** (Interpol Global Complex for Innovation), které má být v roce 2014 otevřeno v Singapuru a má pomoci analyzovat a vyšetřovat kybernetické útoky (151).

Kaspersky Lab „The „Icefog“ APT: A Tale of Cloak and Three Daggers“. Studie vydaná 26.9.2013 ukazuje Operaci Icefog jako kybernetickou kampaň, která probíhá již od roku 2011 a cílí na vládní soukromé společnosti z oblastí vojenství, dopravy, komunikací, průmyslu atd. Kampaň cílí na subjekty v Japonsku a Jižní Koreji a možná i na západní společnosti. Šíří se přes cílené phishingové e-maily se škodlivými odkazy nebo přílohami, zejména dokumenty HWP používanými hlavně v Koreji, a využívá špionážní backdoor pro získávání dat (dokumenty, přístupové údaje atd.). Po získání dat je napadený systém opět malwaru zbaven. Zatím byly objeveny verze pro Windows a Mac OS (155; 156).

Hidden Lynx – jedna z nejvyspělejších skupin operující z čínského kybernetického prostoru. Společnost **Symantec** aktualizovala 26.9.2013 zprávu zaměřenou na hackerskou skupinu Hidden Lynx. Podle zjištění společnosti se jedná o vysoce profesionální skupinu čítající několik desítek členů, která využívá nejmodernější postupy a kombinuje různé typy útoků pro získání přístupu k požadovaným datům. Skupina operuje z čínského kybernetického prostoru a pravděpodobně funguje jako nájemná služba. Vyznačuje se vysokou flexibilitou, schopností rychle útoky modifikovat a využíváním neznámých zranitelností. Cílem skupiny se staly již stovky nejrůznějších společností a vládních institucí (211; 212).

Nová legislativa v boji proti kybernetické kriminalitě. Evropský parlament vydal v červenci 2013 novou **směrnici zaměřenou na boj proti kybernetické kriminalitě**. Směrnice zpřísňuje tresty odnětí svobody pro kybernetické zločince, zaručuje rychlou pomoc ostatních států v případě rozsáhlého kybernetického útoku a zlepšuje komunikaci a výměnu informací při vyšetřování kybernetické kriminality. Nově také definuje další kybernetické zločiny, jako je budování a provozování botnetů, krádeže důvěrných dat nebo používání nástrojů, které

umožňují kybernetickou kriminalitu. Prosazuje také tvrdý postup proti využívání kybernetické špionáže nebo hackování v konkurenčním boji mezi společnostmi. V případě kybernetického útoku, budou muset členské státy Evropské unie reagovat na naléhavé žádosti o pomoc během osmi hodin. Na implementaci směrnice do národních právních systémů mají členské státy dva roky (122; 123).

Spolupráce **Europolu a Interpolu** na poli kybernetické bezpečnosti byla iniciována na dvoudenní konferenci ve dnech 24.-24.9.2013 v Haagu, Nizozemí. Následující konference se budou konat střídavě každý druhý rok v Haagu a Singapuru. Konference je zaměřena na další rozšíření spolupráce sdružující manažery bezpečnostních jednotek zaměřených na boj proti počítačové kriminalitě. Slovy jednoho z účastníků (Noboru Nakatani, výkonný ředitel Interpolu, Globální komplex pro inovace), je počítačová kriminalita mezinárodním zločinem a vyžaduje globální řešení na univerzálních hodnotách. Žádný národ, žádná mezinárodní organizace nemůže tento problém vyřešit samostatně. Potřebujeme globální alianci pro boj proti počítačové kriminalitě (128; 129; 147; 148).

Europol se ve své zprávě SOCTA 2013 (130) zaměřené na vážný a organizovaný zločin mimo jiné zabývá otázkou kybernetické kriminality. Hlavním cílem zločinců je v současné době získání údajů pro podnikání podvodných finančních transakcí buď pomocí phishingu, s využitím malwaru, nebo klasickým hackováním. Stále častěji se dnes zaměřují na poskytovatele služeb a správce databází, kde mohou získat mnohem větší objemy dat. Dle statistických odhadů je nahlášeno pouze 30 % z celkového objemu případů kyberkriminality a kybernetičtí zločinci nejčastěji pocházejí z rusky mluvících zemí. Vzrůstající riziko představuje hlavně rozvoj používání mobilních zařízení a cloudových služeb ve firemním prostředí. Kvůli vyšším rychlostem internetu a dostupným službám online úložišť, P2P sítí, šifrování a anonymizace je stále složitější postihovat závažné zločiny související se zneužíváním dětí. Spolu s rozvojem online plateb se objevuje stále více případů zneužití údajů o platebních kartách. Do budoucna lze očekávat další nárůst kriminality tohoto druhu kvůli vzrůstající oblibě mobilních plateb a bezkontaktních plateb založených na technologii NFC (Near Field Communication).

„Project 2020 Scenarios for the Future of Cybercrime“ z května 2013, je iniciativou **ICSPA** (the International Cyber Security Protection Alliance) jejímž cílem je předvídání budoucnosti počítačové trestné činnosti, umožňující vládám, firmám a občanům připravit se na výzvy a příležitosti nadcházejících deseti let. Nejedná se o předpovědi budoucnosti, ale o možné stavy budoucnosti, soustředící se, na dopady počítačové kriminality z pohledu běžného uživatele internetu, výrobce, poskytovatele internetových služeb a vlády. Analýza vychází ze současných hrozeb, posudků odborníků ICSPA a rozsáhlým monitoringem horizontu zejména nových technologií. Na tvorbě se podíleli odborníci z mezinárodních organizací, vlád, průmyslu a akademické obce (145).

Plánované rozšíření kybernetické obrany na všechny vlastněné a provozované sítě NATO. Členské státy NATO se poprvé v historii prostřednictvím ministrů obrany zaměřily (Brusel 4.-5.6.2013) na kybernetickou bezpečnost a rozhodly se zvýšit spolupráci a rozšířit zabezpečení všech sítí, které aliance vlastní a provozuje (172; 209).

Mezinárodní společenství se musí probudit do reality kybernetické války. Předseda Mezinárodní telekomunikační unie Hamadoun Toure prohlásil (červen 2013), že v současném světě zuří kybernetická válka. Nejmenoval konkrétní viníky, ale zdůraznil, že kybernetické zbraně jsou snadno dostupné a závažné útoky může podnikat prakticky kdokoli, takže k boji proti kybernetickým hrozbám je třeba široké mezinárodní spolupráce na více úrovních. Mimo jiné zmínil kybernetický útok Ruska proti Estonsku v roce 2007 (44), opakované čínské útoky podporované státem proti USA, prorežimní syrské hackery a trvající konflikt mezi Severní a Jižní Koreou (202).

Nová norma **ISO/IEC 27032:2012** se zaměřuje na kybernetickou bezpečnost. Jejím hlavním cílem je vytvořit standardy pro zachování důvěrnosti, integrity a dostupnosti informací v kyberprostoru. Norma sice definuje kyberprostor jako pojem nadřazený internetu, ale už neuvádí, jaká bezpečnostní rizika jsou unikátní právě pro kyberprostor. Není tedy jasné, jak doplňuje stávající nebo vznikající normy o internetové bezpečnosti, a jaký je její praktický

význam a rozsah působnosti. Je těžké stanovit mezinárodní standardy, které by samy o sobě byly klasifikovány jako riziko informační bezpečnosti, ačkoli se ke standardu nevztahují (80).

Materiál **NATO CCD COE** (NATO Cooperative Cyber Defence Centre of Excellence) nazvaný "National Cyber Security Framework Manual" (publikovaný dne 6.12.2012) poskytuje detailní informace a hloubkové teoretické rámce pomáhající pochopit různé aspekty národní kybernetické bezpečnosti podle různých úrovní formulace veřejné politiky. Jednotlivé kapitoly vymezují čtyři úrovně řízení – politické, strategické, operační a technické, zaměřené na kybernetickou bezpečnost. Jsou uvedeny příklady relevantních institucí odpovědné za národní kybernetickou bezpečnost, včetně koordinace a politik pro řešení krizového managementu a podobných institutů (20).

Jiným materiálem resp. sérií jsou **FICS1**, **FICS2**, **FICS3** tzv. "Frameworks for International Cyber Security". FICS1 (publikováno v prosinci 2010, upraveno 18.2.2011) je reakcí na rostoucí poptávku mezinárodní počítačové bezpečnostní komunity držet krok s kybernetickými hrozbami. Edice představuje souhrn kybernetické bezpečnosti právních a politických nástrojů přijatý vrcholnými evropskými institucemi (Evropská unie, Rada Evropy, Organizace pro bezpečnost a spolupráci v Evropě) a mezinárodními institucemi (Mezinárodní telekomunikační unie, Organizace pro hospodářskou spolupráci a rozvoj, Organizace spojených národů). FICS2 (publikováno v květnu 2010, upraveno 18.2.2011) poskytuje pohled na judikaturu Evropského soudu pro lidská práva a Evropského soudního dvora a seznámení se s přístupy k ochraně osobních údajů a dokumentům, právními analýzami, radami, legislativními technikami a odbornými diskusemi. FICS3 je sestavením resp. výběrem webových odkazů (aktualizovaných k 19. listopadu 2013) na národní politiky a strategie kybernetické bezpečnosti jednotlivých států (18; 19).

USA vs. EU – diskuse v kauze špionážních aktivit ze strany USA. Evropské země, především pak Německo a Francie, požadují (červenec 2013) po Spojených státech vysvětlení odtajněného programu sledování a špionáže. Spojené státy nejdříve poukazovaly na to, že sledování ostatních zemí je cílem každé národní tajné služby, ale postupně svůj postoj

přehodnocují a začínají uznávat vážnost situace, která by mohla poznamenat vztahy a ohrozit nejrůznější vyjednávání se zeměmi EU. Vláda USA se chystá detailně probrat konkrétní témata s evropskými partnery (230; 232).

Francie: Státní monitoring internetové a telefonické komunikace. Francouzská vláda, která kritizuje USA za kontroverzní (protiteroristický) program **Prism**, sama čelí kritice za vlastní utajený program sledování telefonní a internetové komunikace. Informace o tajném protiteroristickém a kriminalistickém programu francouzské tajné služby DGSE přinesl deník Le Monde (červenec 2013), který také uvedl, že program nepodléhá žádné kontrole, a je tedy snadno zneužitelný ke sledování kohokoli (161).

4.2 Sousední státy – Německo, Polsko, Rakousko, Slovensko

Polský CERT zveřejňuje zhruba jednou měsíčně studie mající úzkou souvislost s polským internetovým prostorem – případy infikování webových stránek, zneužití národních domén, statistické zprávy, útoky proti polským vládním webům, ale i významné tituly, které by se mohly týkat polských uživatelů (48).

Polská organizace **NASK** (167), podobně jako i jiné instituce, zveřejňují odlišné informace v mateřském a anglickém jazyce. V polštině jsou mezi aktualitami např. informace k bezpečnostní konferenci s účastí zástupců Interpolu (říjen 2013), dále NASK jako partner Evropského měsíce kybernetické bezpečnosti (říjen 2013), setkání expertů evropských států na téma bezpečnosti dětí a mládeže na Internetu (září 2013). V angličtině je informací poněkud méně – ze srpna 2013 ukončení smlouvy s jedním ze svých partnerů zodpovědný za nakládání s nebezpečnými internetovými adresami, z května 2013 obnovení certifikátu podle ISO 9001 (systém managementu řízení kvality), a z ledna 2013 vypnutí nebezpečných Virut botnet domén (domény používané pro kriminální aktivity). Stránky CERT jsou aktuálnější a bez rozdílu informací zveřejňovaných v polštině a angličtině a zejména obsahově zaměřené na kybernetickou bezpečnost polského Internetu (49; 169).

Polský **CERT.pl** cílí na domény využívané botnetem Virut. Polský správce doménového registru **NASK** převzal (leden 2013) kontrolu nad 23 doménami, které byly zapojeny do šíření a správy botnetu Virut. Ten se již od roku 2006 šíří prostřednictvím přenosných disků a stahování obsahu z internetu a jeho novější verze napadají počítače také prostřednictvím vložených prvků na webových stránkách. Celkem bylo evidováno přes 300 000 nakažených počítačů. Botnet byl využíván pro útoky typu DDoS (Distributed Denial of Service) nebo např. pro šíření spambotu Waledac. Domény byly využívány kromě šíření a řízení malwaru Virut také k šíření dalších nákaz, např. Palevo nebo Zeus. Největší výskyt počítačů infikovaných botnetem Virut je v Egyptě, na Indickém poloostrově a v oblasti Indonésie (168; 214).

Nový rozsah portů využívaných protokolem ZeuS P2P. Malware Zeus nově změnil rozsah portů UDP (User Datagram Protocol) využívaných protokolem GameOver P2P (Peer-to-Peer). Nové verze již nové pásmo standardně využívají a starší verze jsou postupně aktualizovány. Předpokládá se, že tuto změnu vyvolala červnová (červen 2013) zpráva polského týmu CERT, ve kterém byla zveřejněna podrobná analýza nástroje Zeus (50).

Příspěvkový blog **CERT.at** není téměř využíván. Poslední informace je z dubna 2013 vztahující se k útokům proti spol. **Spamhaus** (viz dále), tzv. „Special Report: Der Spamhaus/CloudFlare/Stophaus Denial of Service Angriff“[4], o kterém psala i většina světových mediálních společností. Zpráva je shrnutím skutečností k této události z pohledu rakouského týmu, který se zapojil do spolupráce s dalšími bezpečnostními týmy. Dále velice zajímavá nabídka blogu několika aplikací pro např. generování histogramů, vyhledávání a analýzu malware potencionálně infikovaného systému Microsoft Windows nebo interaktivní analýza pomocí grafu generující systémové logy (38; 42).

Organizace **Spamhaus** (poskytovatel antispamových seznamů blokovaných internetových adres) se stala v březnu 2013 terčem masivního útoku typu DoS (Denial of Service), který díky zesílení přes DNS (Domain Name System) servery dosahoval rekordní intenzity až 300 Gb/s. Společnosti Spamhaus se dařilo dlouhodobému útoku poměrně dobře odolávat hlavně díky podpoře od velkých společností (např. Google). Útok mohlo pravděpodobně spustit zařazení dánské hostingové společnosti Cyberbunker na seznam serverů šířících spam. Cyberbunker podle spol. Spamhaus poskytuje hosting i kyberkriminálním organizacím z východní Evropy a Ruska. Společnost Cyberbunker sice obvinění popřela, ale vyhrazovala se proti tomu, že by právě společnost Spamhaus měla mít právo rozhodovat o tom, koho je třeba na internetu blokovat. Útoky DDoS takto velkého rozsahu na DNS servery mohou vést ke snížení dostupnosti i ostatních služeb a k celkovému omezení provozu na internetu. Projekt Spamhaus (the Sapmhaus Project) je mezinárodní nezisková organizace, jejímž posláním je monitorování internetových spamových operací a zdrojů, zajištění spolehlivé antispamové ochrany internetových sítí v reálném čase, spolupráce s vyšetřovacími orgány

[4] Zpráva CERT.at je dostupná na: http://www.cert.at/static/downloads/specials/20130408-cert.at-report-ddos.pdf.

na identifikaci a sledování zločineckých (spamových a malwareových) skupin po celém světě, včetně lobování u vlád pro účely legislativní efektivní antispamové ochrany. Organizace byla založena v roce 1998 se sídly v Ženevě a Londýně. Databáze jsou používány u většiny poskytovatelů emailových služeb, organizací, univerzit, vlád a vojenských sítí (13; 207; 208).

Slovenský CSIRT je na tom podobně jako český – jednou týdně zveřejňuje zranitelnosti, aktualizace zejména produktů nadnárodních společností jako např. Microsoftu, Adobe, Google. Samotný web je určitě svým obsahem důstojnější než český. Nejvýraznějším prvkem je určitě graf s nahlášenými incidenty za rok 2013, který je barevně a procentuálně rozdělený do sedmi typů provedených útoků. Určitě stojí za zmínku odkaz na virusový radar provozovaný původem slovenskou spol. Eset, spol. s r. o. (117) monitorující a statisticky analyzující počítačové infiltrace šířící se prostřednictvím elektronické pošty (nejrozšířenější forma možnosti infikování počítače s přiloženou infikovanou přílohou nebo odkazem na infikovaný web) a Online Scanner stejné společnosti. Dalšími informacemi pro běžného čtenáře jsou informace o volně dostupných antivirových řešeních, kde jsou v několika větách uvedeny vždy jednotlivé produkty včetně odkazů na domovské stránky. Jsou popisovány např. Avast! Free Antivirus, AVG Anti-Virus Free Edition, Comodo Antivirus a jiné, včetně dalších 12 samostatných produktů, které tyto společnosti nabízejí jako on-line nástroje jako určitou dostupnou a rychlou alternativu. Webové stránky slovenského CSIRTu jsou určitě jedněmi z **nejpřínosnějších** pro běžného uživatele vůbec (55).

4.3 Jiné členské státy EU, státy mimo EU

Jsou-li zmiňovány kybernetické útoky velkého rozsahu proti národní infrastruktuře, je Estonsko zmiňováno jako vzorový příklad. V dubnu roku 2007 **estonský CERT** upozornil na kybernetické útoky cílené proti estonským webům (viz Obrázek č. 3), které byly přístupné pouze z estonského internetového prostoru, ze zahraničí byly nedostupné. Bylo potvrzeno, že útoky jsou vedeny ze zahraničí (44). Studie (z května 2012) Institutu informatiky Univerzity v Talinu nazvaná „Cyber Security in Estonia: Lessons from the Year 2007 Cyberattack" analyzuje s odstupem pěti let změny v oblasti kybernetické bezpečnosti v Estonsku. Útoky mající politický podtext (přemístění sochy bronzového vojáka z centra města na nedaleký vojenský hřbitov) trvaly 22 dní (17.4-18.5.2007). Cílem útoků byly webové stránky estonských vládních institucí, škol, bank, poskytovatelů internetových služeb, mediálních agentur a soukromých vlastníků.

Obrázek č. 3: Upozornění estonského CERTu na cílené kybernetické útoky. Dostupné na: https://www.ria.ee/malicious-cyber-attacks-against-estonia-come-from-abroad (44).

Rozsah, rozmanitost a různorodost cílů těchto útoků nesou známky nacionalistického pozadí. Ačkoli ruská strana odmítla spolupracovat na vyšetřování útoků, a mnoho indicií poukazuje na útočníky, příznivce Ruské federace (ruský jazyk na pozadí nežádoucího provozu) zůstává podle některých odborníků neprokázaná souvislost s ruskou vládou a jejím tichým souhlasem s útoky (44; 157).

Estonsko je dnes vůdčí zemí Evropské unie v oblasti kybernetické bezpečnosti. Je sídlem **NATO CCD COE** (viz kapitola 3.2) a od roku 2012 sídlem Evropské agentury pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva. To vše je důsledkem útoků z roku 2007, následným uchopením a implementací postupů vytvářející rámec bezpečnostních politik, které jsou užitečné i pro jiné země.

Jiný příklad kybernetických útoků proti Gruzii z července roku 2008 obsahuje zpráva **gruzínského** vysokoškolského týmu **CERT** zaslaná estonskému týmu CERT. Došlo k pozastavení veškerých bankovních operací, poskytovatelé internetových služeb měli problémy s přesměrováním webových stránek, státní instituce přemístily provoz webů na zahraničí servery. Došlo k zahlcení internetového provozu prostřednictvím cílených DDoS útoků (43).

Bylo-by možné vyjmenovat desítky příkladů kybernetických útoků proti digitální infrastruktuře států celého světa. Nejvyšší počet těchto útoků je směrován proti USA resp. subjektům amerického původu zejména čínskými, státem podporovanými skupinami (viz studie spol. Kaspersky Lab, Symantec a Mandiant) zaměřující se zejména na průmyslovou špionáž. Poslední roky stále aktivnější skupiny aktivistů, tzv. **hacktivists** (Anonymous), propagující svůj názor proti státním institucím celého světa (nejčastěji DDoS útoky proti webům nebo jejich defacement – znetvoření obsahu), ve stále trvajícím syrském konfliktu známá provládní **SEA** (The Syrian Electronic Army) útočící zejména proti americkým a britským mediálním agenturám popisující boje v Sýrii v neprospěch režimu prezidenta Bašára al-Asada, dnes již prokázaný americko-izraelský projekt malware **Stuxnet** (objevený

v roce 2010), namířený proti íránskému jadernému programu nebo tzv. operace **Aurora**[5] (z přelomu roku 2009-2010) namířená proti největším americkým společnostem (např. Adobe Systems, Google, Yahoo) ze strany čínských příznivců a mnoho dalších útoků.

Nejvýznamnějšími státy na poli kybernetické bezpečnosti jsou Čína, Rusko a USA. Čínský internetový prostor je nejčastěji uváděn, jako místo odkud jsou podnikány kybernetické útoky proti USA. Potvrzují to opakovaně nejen studie uznávaných bezpečnostních společností (včetně vyšetřování tzv. digitálních stop po různých útocích), ale i nejvyšší představitelé zpravodajských a bezpečnostních složek, které úzce s těmito společnostmi spolupracují. Ruský internetový prostor je zaměřený zejména na kriminální činnosti spojené s krádežemi identit, osobních dat zejména bankovních. Rusko a USA se v červnu 2013 dohodly na rozšíření transparentnosti v oblasti kybernetické bezpečnosti. Týmy CERT obou zemí a ministerstva obrany budou mnohem intenzivněji spolupracovat a vyměňovat si informace. Také bylo ustanoveno neustálé spojení obou zemí, které zajistí včasné řešení případných kybernetických krizí. Armády obou zemí si také začaly vyměňovat neutajené dokumenty týkající se informačních a komunikačních technologií. Nová úroveň spolupráce by měla zajistit lepší transparentnost a snížit rizika kybernetických hrozeb (237).

Narušení důvěry internetu zpravodajskými službami USA a Velké Británie. Aféra s „odtajněnými dokumenty“ Edwardem Snowdenem nabírá konkrétní rysy (září 2013). Podle uvolněných dokumentů **E. Snowdena** agentury americká NSA (The National Security Agency) a britská GCHQ (The Government Communications Headquarters) nejen odposlouchávají a prolamují šifrovací programy, ale podílejí se přímo i na programování zranitelností. Mimo jiné jsou jmenovány: 10 let trvající program zabývající se luštěním šifrovacích metod a technologií s velkým průlomem v roce 2010; 250 milionů USD

[5] Pozadí útoků resp. co jim předcházelo – 06/2009 byla objevena nedostatečná cenzura čínské verze vyhledávače Google, kdy se ve výsledcích vyhledávače objevily pornografické stránky, které mají být nepřístupné; objevují se spekulace o spolupráci čínské vlády a společnosti Apple na určité represivní obchodní strategii; Google oznamuje odchod z čínského trhu, který se ovšem neuskutečnil; čínští zaměstnanci Google používají verzi Internet Explorer 6, která je zranitelná a přes kterou dochází k počátečním útokům – Google má přitom vlastní prohlížeč Chrome; první informace hovořily o útocích přes infikovanou přílohu v aplikaci Adobe, ale zranitelnost prohlížeče od Microsoftu se stala závažnou natolik, že ji samotný Microsoft potvrdil, jako kritickou při těchto útocích. Dostupné na: http://blogs.mcafee.com/corporate/cto/operation-aurora-hit-google-others.

utrácených NSA ročně na „nenápadné ovlivňování“ a vkládání zranitelností a zadních vrátek do produktů společností s novými technologiemi; snahy britského GCHQ vyvinout způsoby, jak monitorovat šifrované zprávy u Hotmail, Google, Yahoo, a Facebooku. Obě agentury tyto a jiné činnosti nepopírají – naopak tvrdí, že pro svou práci schopnost dešifrovat potřebují. Odborníci je však obviňují z napadení práv uživatelů internetu, a internetu jako takového (200; 231; 233).

Společnosti Google a Microsoft podaly (srpen 2013) žaloby na vládu USA. Společnost Microsoft oznámila,[6] že žaloby byly podány, jelikož již několik měsíců trvá spor s federální vládou USA o jejich právu zveřejnit více informací o počtech vládních žádostí o soukromá data uživatelů. Microsoft a Google jsou znepokojeni neochotou vlády umožnit zveřejnění těchto dat souvisejících s pokyny programu **FISA** (Foreign Intelligence Surveillance Act). Obě společnosti zveřejnily počty takových žádostí od místních, státních, i federálních institucí. Tvrdí však, že je jejich povinností zveřejnit i další informace. Vláda naopak trvá na tom, že takové zveřejnění by mohlo poškodit bezpečnostní zájmy země (5).

Americká NSA usiluje o **sdílení informací v reálném čase** s dalšími agenturami. Šéf americké NSA veřejně usiluje (září 2013) o přijetí legislativy, která by americkým bezpečnostním službám umožnila sdílet získané informace v reálném čase se společnostmi ze soukromého sektoru a případně i s cizími bezpečnostními agenturami. Jedině tak mohou být výsledky analýzy získávaných dat efektivně využity v boji proti závažným hrozbám (238).

Britský ministr kanceláře vlády Francis Maude informoval dne 12.9.2013 o **nastavení spolupráce** britského CERT (GovCertUK) a indického CERT (CERT-In). Na pozadí spolupráce stojí zkušenosti z olympijských her v Pekingu v roce 2008, „New Delhi Commonwealth Games“ z roku 2010, olympijských her v Londýně v roce 2012 a v současnosti se rozšiřující spolupráce s brazilskými bezpečnostními odborníky z důvodu konání olympijských her v roce 2016 v Brazílii. Pokračuje tak podpora spolupráce více

[6] Oficiální vyjádření spol. Microsoft je dostupné on-line na http://blogs.technet.com/b/microsoft_on_the_issues/archive/2013/08/30/standing-together-for-greater-transparency.aspx

zainteresovaných stran umožňující model správy internetu navržený na světovém summitu OSN v roce 2005 - the UN World Summit on the Information Society in 2005 (140).

The **CISP** (Cyber-security Information Sharing Partnership) umožňuje britské vládě a průmyslu sdílení informací o aktuálních hrozbách včetně řízení incidentů. Po úspěšném pilotním projektu, kterého se zúčastnilo 160 společností z pěti odvětví - obrana, finance, farmacie, energetika a telekomunikace - je CISP otevřen dalším společnostem v rámci kritické národní infrastruktury a v druhé fázi rozšiřuje služby pro malé a střední podniky (141).

Spojení britských „The Police Central e-Crime Unit“ a SOCA (the Serious Organised Crime Agency) vytváří nově formovanou **NCA** (National Crime Agency) od října roku 2013. NCA se stane primárním orgánem pro boj se závažným a organizovaným zločinem. I přes omezený rozpočet se bude zaměřovat na organizovaný zločin, ekonomické zločiny, pohraniční zabezpečení, zneužívání dětí a jejich ochranu online, a kybernetickou kriminalitu. Jednotka bude reakcí na kybernetické trestné činnosti nejen ve Velké Británii, ale i na mezinárodní úrovni, jejímž cílem bude předcházení počítačové trestné činnosti vedoucí k ochraně občanů Velké Británie a komerční a národní infrastruktury (142; 179).

Spolupráce amerických univerzit a NSA na společném programu kybernetických operací „Cyber-ops program“. Tato spolupráce (zveřejněná v září 2013) navazuje na snahu NSA a ostatních agentur přejít z aktivní obrany do aktivního útoku tím, že si vychová odborníky od studentských let – včetně letních brigád a bezpečnostních prověrek. NSA nediktuje školám, co mají studenty učit. Školy však obvykle staví studijní programy zejména na předmětech teorie, programovacích jazyků, architektury různých typů sítí, zabezpečení softwaru, hardwaru, a základech radiových, bezdrátových a mobilních sítí (234).

Americká FBI spustila (červenec 2013) nový bezpečnostní portál **iGuardian** pro ohlašování kybernetických hrozeb nebo útoků v reálném čase. Členské společnosti (kterých je na 58 000) sítě InfraGuard mají portál využívat k efektivnějšímu sdílení informací o rizicích a útocích. Výsledky analýz malwaru a jednotlivých útoků mají pak pomoci ostatním členům lépe

nastavit bezpečnost svých systémů. FBI postupně hodlá zapojit do programu další subjekty a zpřístupnit informace soukromým společnostem (135; 146).

Austrálie prezentovala nově vznikající program pro kybernetickou bezpečnost. Studie nazvaná „The emerging agenda for cybersecurity“ vydaná 16.7.2013 **ASPI** (Australian Strategic Policy Institute) se soustředí na vytváření nového programu pro kybernetickou bezpečnost, jehož součástí je i vytvoření australského centra kybernetické bezpečnosti ACSC (Australian Cyber Security Centre), které sdružuje celou řadu dalších složek a úřadů pro efektivnější obranu proti kybernetickým hrozbám. Austrálie tak chce následovat příkladu Spojeného království a USA (1).

Prezident USA Barack Obama věří (červen 2013) ve **strategickou konverzaci** s Čínou na téma kybernetické bezpečnosti. Americký prezident věří, že si Čína postupně přizná odpovědnost za situaci v kyberprostoru a bude se s USA účastnit na jeho regulaci. I když čínská vláda dál odmítá jakoukoli spojitost s čínskými hackerskými skupinami, které kradou důležité informace americkým společnostem, přeci jen je nové vedení ČLR mnohem přístupnější rozhovorům ohledně klíčových témat, jako je například také otázka Severní Koreje (205).

Kybernetická bezpečnost je jednou z nejvyšších priorit prezidenta USA Baracka Obamy. Obamova administrativa zařadila kybernetické útoky na první místo v seznamu **globálních bezpečnostních hrozeb**. Vyplývá to z výroční zprávy „Worldwide Threat Assessment of the Intelligence Community“ z března 2013. Podle zjištění je řada klíčových infrastruktur, zejména elektrické sítě, napojena na internet a před kybernetickými útoky chráněna jen minimálně. Zranitelné jsou také banky a finanční instituce a v neposlední řadě weby státní správy a komunálních služeb, včetně hasičských služeb, vodohospodářských a dopravních systémů (15; 152).

Prezident USA B. Obama podepsal (prosinec 2012) „National Strategy for Information Sharing and Safeguarding“, která si klade za cíl zvýšit zabezpečení informací tak, aby k nim

neměly přístup nepřátelské síly, ale zároveň byly snadno přístupné pro instituce hájící státní zájmy. Bílý dům tak chce podpořit spolupráci zainteresovaných subjektů na rychlejším a spolehlivějším systému sdílení informací a na integraci společných postupů a standardů, včetně právního a technického zajištění bezpečnosti informací. Důrazem na zabezpečení dat chce předkládaná strategie ochránit soukromí, práva a svobody občanů. Zdokonalení sdílení informací má potom pomoci efektivněji prosazovat a bránit národní zájmy (236).

Centrum FBI pro hlášení internetové kriminality **IC3** (Internet Crime Complaint Center) uvádí (květen 2013) ve své zprávě „2012 Internet Crime Report“, že obdrželo skoro 290 000 hlášení kybernetických zločinů, které způsobily škody za více než 525 milionů USD. IC3 řešilo nejrůznější incidenty od podvodných obchodů, telefonátů a e-mailů přes phishing až po ransomware a pomáhalo i při jejich vyšetřování a soudním řešení. Centrum se také snaží zvyšovat povědomí veřejnosti a informovat příslušné orgány o nově objevených podvodech (131; 144).

Výroční zpráva britské **ICS** (The Intelligence and Security Committee) „Annual Report 2012-2013“ z července 2013 věnuje kybernetické bezpečnosti jednu kapitolu, ve které mimo jiné poukazuje na hrozbu kybernetických útoků, která je v současnosti na nejvyšší úrovni a očekává se, že dále ještě poroste. Upozorňuje i na státy (zmiňovány Čína a Rusko) podporované a sponzorované útoky na různé cíle zejména finanční instituce a energetické společnosti. Kybernetická bezpečnost bude i nadále významnou hrozbou v následujících letech (149).

Microsoft Digital Crimes Unit ve **spolupráci** s FBI, Europolem a dalšími institucemi významně narušila (červen 2013) činnost obřího botnetu Citadel, který čítal až pět milionů infikovaných počítačů po celém světě a útočil na platební služby světových bank a finančních společností. Celkem se podařilo zrušit přibližně 1 400 dílčích sítí, které za uplynulých 18 měsíců odhadem způsobily škody ve výši 500 milionů dolarů. Vyšetřovatelé se tak přiblížili o krok blíž k dopadení tvůrce botnetu a ostatních členů zločinné organizace (163; 203).

Společnosti Microsoft se podařilo sjednat (říjen 2012) dohodu s čínským **CERT** (Chinese Computer Emergency Response Team, CN-CERT) a čínským provozovatelem domény 3322.org, která poskytovala hosting asi 70 000 škodlivých subdomén. Součástí dohody je revize služeb 3322.org, blokování všech připojení k subdoménám figurujícím na vypracovaném seznamu, přidávání nově identifikovaných škodlivých subdomén do seznamu a spolupráce na identifikaci jejich provozovatelů. Společnost Microsoft doposud úspěšně filtrovala jednotlivá připojení, tak aby byl co nejméně dotčen provoz bezpečných subdomén. IP adresy nakažených počítačů pak dále delegovala jednotlivým poskytovatelům, aby mohli být majitelé nakažených zařízení varováni. Likvidací botnetu Nitol se tak podařilo přerušit činnost asi 500 malwarových operací. V rámci vyšetřování byl také objeven nový způsob infikování počítačů, kdy se kybernetičtí zločinci spolčují s některými pochybnými distributory a instalují malware do počítačů ještě předtím, než se dostanou k zákazníkům (162).

Několik nizozemských bank a dalších institucí se stalo (duben 2013) terčem masivních útoků typu DDoS, které dočasně vyřadily z provozu různé webové stránky včetně stránek internetového bankovnictví. Zasažen byl také digitální podpisový systém DigiD, který přes deset milionů Nizozemců využívá ke komunikaci se státní správou. Ministerstvo vnitra ve spolupráci s policií a týmem **CERT** incident vyšetřuje (194; 201).

Rumunská tajná služba SRI zveřejnila (březen 2013) podezření, že za vývojem a použitím malwaru MiniDuke stojí státní organizace některé země. Malware infikoval vládní a výzkumné instituce a kradl citlivá data. Podle SRI mohl napáchat větší škody než dříve objevený špionážní malware Red October, který se zaměřoval na východoevropské země a státy bývalého sovětského bloku. SRI spolupracuje na dalším vyšetřování malwarové operace MiniDuke ve spolupráci se speciální telekomunikační službou STS a **rumunským CERT** (204).

Nezávislá komise složená z předních odborníků na mezinárodní právo zpracovala (březen 2013) otázku kybernetických konfliktů vzhledem k mezinárodním smlouvám. Odborníci

se zabývali otázkou hodnocení kybernetického útoku a došli k závěrům, že například útok s použitím malwaru Stuxnet na íránská jaderná zařízení, za nímž stojí USA a Izrael, lze označit za akt síly. Otázkou ale zůstává, zda mohl představovat „ozbrojený útok“, který by pak byl z hlediska mezinárodních smluv (např. Ženevských konvencí) považován za záminku k ozbrojenému konfliktu nebo válce. Naopak kybernetický útok vedený v rámci otevřeného vojenského konfliktu je dle zprávy jednoznačně možné považovat za ozbrojený útok a jeho původci se stávají přímými účastníky konfliktu. Nejspornější otázkou ale i nadále zůstává nanejvýš problematické určování skutečného původce útoku (24; 235).

Indický ministr komunikací a informačních technologií uvedl (únor 2013), že indická vláda pracuje na vytvoření politiky kybernetické bezpečnosti, která by lépe reagovala na kybernetické hrozby a chránila občany. **Indický** bezpečnostní tým **CERT-In** již nyní monitoruje provoz na internetu a hledá případné zločinné aktivity. Ministr také prohlásil, že se bude intenzivně zabývat veřejnou osvětou v této oblasti a ochranou obyvatel před kybernetickými útoky. Zároveň zdůraznil nutnost mezinárodních smluv, které by umožnily stíhání útočníků i mimo Indii (206).

Ruská kybernetická špionáž proti Gruzii v roce 2011. **Gruzínskému CERT** se podařilo odhalit rozsáhlou špionážní síť na počítačích patřících vládním institucím. Síť byla vytvořena za pomoci sofistikovaného malwaru umístěného na stránky s vysokou pravděpodobností návštěvy cílového uživatele. Malware vyhledával a kradl citlivé dokumenty a využíval webové kamery, mikrofony a keyloggery pro účely špionáže. Gruzijskému týmu se dokonce podařilo úspěšně nastražit honeypot (nástroj pro odchyt malwaru) a získat kontrolu nad počítačem jednoho z hackerů. Kromě poskytovatele připojení, e-mailové adresy a dokumentů týkajících se vývoje malwaru získali dokonce i videonahrávku hackera přes webovou kameru. Spolu s dalšími materiály byly tak získány důkazy kybernetické špionáže vedené proti Gruzii ruskou hackerskou skupinou s napojením na ruskou vládu (164; 246)

Kybernetický prostor má být zařazen mezi tradiční válečné sféry. Tedy mezi moře, zemi a vesmír, prohlásil (říjen 2010) náměstek ministra obrany USA William J. Lynn III. Toto

prohlášení navazuje na vznik úřadu **U. S. Cyber Command** v květnu 2010 a na jeho dohody s Ministerstvem obrany a Ministerstvem pro vnitřní bezpečnost z poslední doby. Informační technologie poskytují kritické výhody ve všech válečných sférách a je proto třeba kybernetický prostor hájit (241).

DDoS útoky na Myanmar (Barma) byly **patnáctkrát větší** než útoky na Estonsko v roce 2007 (viz výše). Útoky DDoS s nevyžádanými údaji o velikosti až 15 Gb/s na hlavního (jediného) poskytovatele internetu Myanmaru MPT (The Myanma Posts and Telecommunications) paralyzovaly část infrastruktury země. Počátek útoků byl datovaný před termín všeobecných voleb (7.11.2010 – stanovených místním vojenským režimem). Objevují se spekulace o tom, že útok spustila sama junta k manipulaci s výsledky voleb. Jiné teorie spekulují se zdrojem útoku ze zahraničí (10; 228).

Situace kolem postupného zveřejňování dokumentů E. Snowdena prostřednictvím významných mediálních agentur (viz výše) nemá daleko k jiné, avšak neméně významné události z roku 2010 – zveřejnění dokumentů **WikiLeaks**.

WikiLeaks zveřejnila 400 000 dokumentů z války v Iráku. V dokumentech je mimo jiné poukázáno na to, že američtí velitelé ignorovali důkazy o mučení iráckou policií a iráckými vojáky a také, že více než 15 000 civilistů zahynulo v incidentech, o kterých nebyly dříve poskytnuty informace. Databáze pokrývá období 2004-2009 (229; 244; 245).

Přehledná aktualizace časové posloupnosti „The WikiLeaks drama: A timeline“ od 28.11.2010 (první zveřejnění informací několika zahraničními mediálními agenturami) do 8.12.2010 (DDoS útoky příznivců WikiLeaks) s nejdůležitějšími informacemi a s odkazy podrobně zveřejňovaných událostí společnosti CSO (199).

4.4 Česká republika

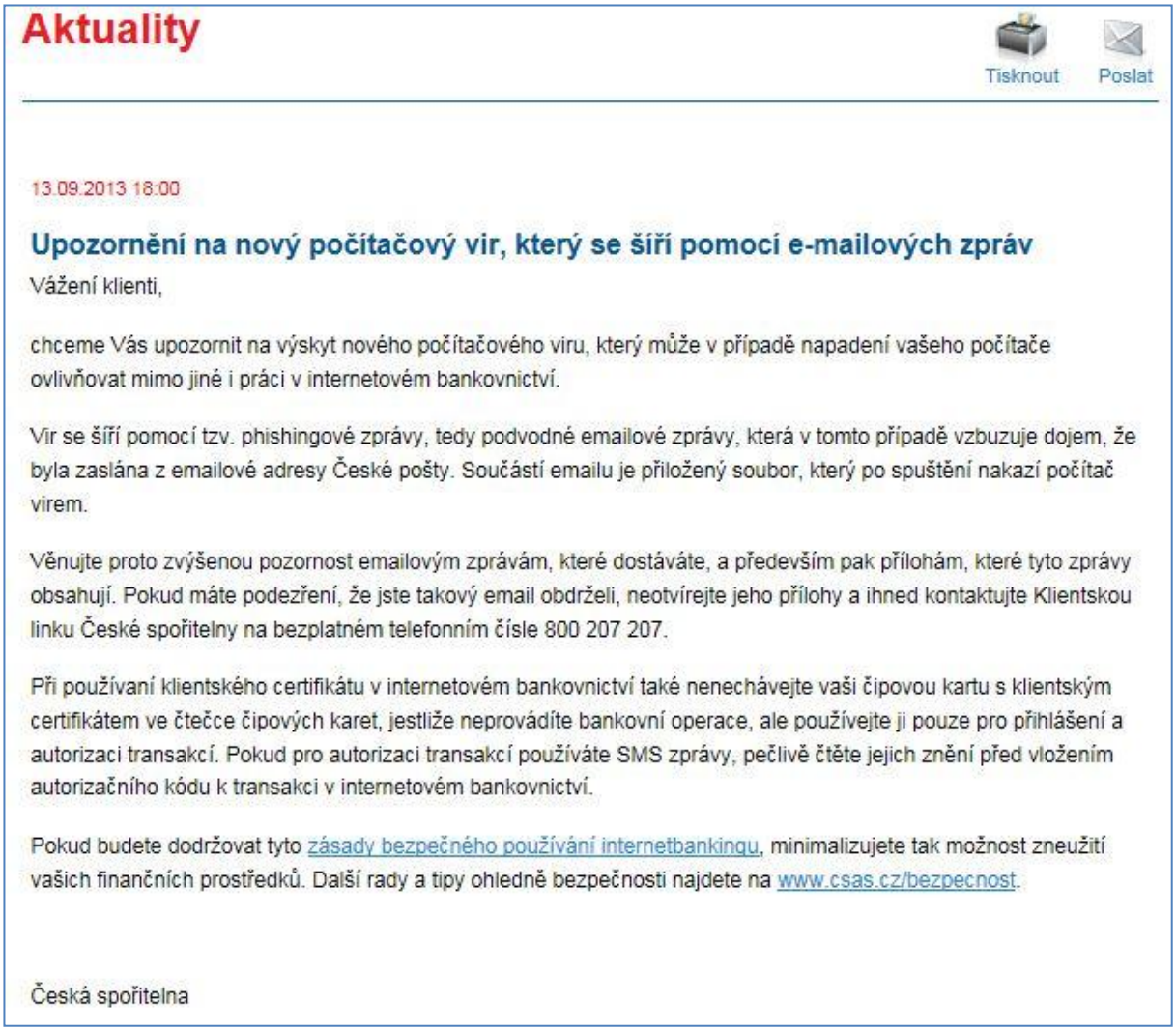
Evropská unie v rámci zvýšení povědomí kybernetické bezpečnosti občanů pořádá od října roku 2011 kampaň nazvanou **European Cyber Security Month** opakující se v měsíci říjnu daného kalendářního roku – v roce 2013 již potřetí. Projekt cílí na několik klíčových témat a událostí s globálním dosahem. Byl podpořen agenturou ENISA a Evropskou komisí. Česká republika s výjimkou tiskového brífinku pořádá konferenci prostřednictvím Národního centra bezpečnějšího internetu (neplést s Národním centrem kybernetické bezpečnosti tzv. vládní CERT České republiky.) Konference „Kyberpsycho" – prevence, řešení a právní souvislosti elektronického násilí je zaměřena na mladé uživatele internetu a mobilních technologií. Na webu Národního centra bezpečnějšího internetu je uváděno, že dojde k sérii akcí a iniciativ v rámci této kampaně, ale kromě jednodenní konference zde žádné jiné aktivity prezentovány nejsou (k datu 1.10.2013). Na základě těchto aktivit dojde (podle popisu) k prohloubení komunikace a spolupráce mezi zainteresovanými subjekty. Kalendář akcí na říjen ukazuje šest jednodenních akcí, na listopad pět, v září jich bylo devět. Je-li měsíc říjen evropským měsícem kybernetické bezpečnosti, lze předpokládat, že dojde k navýšení aktivit Národního centra bezpečnějšího internetu (záštitu nad kampaní převzal ředitel vládního CERTu České republiky pana Mgr. Rohel). Podle kalendáře akcí to zatím tak nevypadá (106; 107; 116; 180; 181; 182; 183; 188).

Na webu národního **CSIRTu** je umístěna k 17.10.2013 novinka „Doporučení pro případ napadení DoS či DDoS útokem" které vypracovalo **NCKB** s partnery ze státní, soukromé a akademické sféry na základě DDoS útoků z dubna 2013 (viz dále). Samotný dokument obsahuje několik základních pojmů uvedené analýzy s krátkým vysvětlením. Vysvětlení pojmu „kybernetický útok" je odlišný od vysvětlení, které je součástí Výkladového slovníku kybernetické bezpečnosti, který je na webu NCKB ke stažení také (153). NCKB resp. zpracovatel (který měl být k tomu veden) zpravované analýzy nereflektoval pojem, který je dnes jedním z nejčastěji používaných v souvislosti s jakoukoli charakteristikou uskutečněného „**kybernetického útoku**". Další slovo v obsahu předchozího vysvětlení „**autorizace**" (spojení s přístupovými právy) by možná měla být nahrazena slovem

„**autentizace**“ (ověření identity) vycházíme-li z již zmiňovaného Výkladového slovníku a pochopení z pozice běžného uživatele. Autor analýzy uvádí odkazy na použité zdroje z období let 1998, 1999, 2000 a 2006. Je-li seznam zdrojů kompletní, tak nám NCKB prezentuje materiál, jehož obsah je v některých bodech sedm až 15 let starý. Technologický (počítačový) vývoj se mění každým rokem, tak musíme my, běžní uživatelé, kteří mají snahu dozvědět se něco více o počítačové bezpečnosti, věřit tomu, že zpracovaný materiál předložený nejvyšší státní autoritou na problematiku kybernetické bezpečnosti není svým obsahem částečně zastaralý. Materiál sám o sobě není ničím, co by zkušený pracovník v problematice počítačové bezpečnosti nevěděl nebo minimálně již měl mít základní povědomí. Možná jsou zde zveřejňované informace určeny pro jiný okruh „čtenářů“ než je běžný uživatel. Potom by však postrádala smysl jedna z hlavních činností NCKB popisovaná jako „osvěta a podpora vzdělávání v oblasti kybernetické bezpečnosti“ (65; 185; 187). Pro návštěvníka webu NCKB tak vzrůstá míra **nedůvěry**, zde v práci nejednou zmiňovaná.

CSIRT.CZ varoval před phisingovou zprávou cílenou na uživatele **České spořitelny**. Bohužel datum zveřejnění je k datu 1.10.2013 (viz Obrázek č. 4). Samotná Česká spořitelna zveřejnila toto upozornění již 13.9.2013 (viz Obrázek č. 5).

Obrázek č. 4: Opožděné varování CSIRT.CZ před phishingovou zprávou. Dostupné na: http://csirt.cz/page/1633/csirt.cz-zachytil-phishingovou-zpravu-smerujici-na-uzivatele-ceske-sporitelny (68).



Aktuality

Tisknout Poslat

13.09.2013 18:00

Upozornění na nový počítačový vir, který se šíří pomocí e-mailových zpráv

Vážení klienti,

chceme Vás upozornit na výskyt nového počítačového viru, který může v případě napadení vašeho počítače ovlivňovat mimo jiné i práci v internetovém bankovnictví.

Vir se šíří pomocí tzv. phishingové zprávy, tedy podvodné emailové zprávy, která v tomto případě vzbuzuje dojem, že byla zaslána z emailové adresy České pošty. Součástí emailu je přiložený soubor, který po spuštění nakazí počítač virem.

Věnujte proto zvýšenou pozornost emailovým zprávám, které dostáváte, a především pak přílohám, které tyto zprávy obsahují. Pokud máte podezření, že jste takový email obdrželi, neotvírejte jeho přílohy a ihned kontaktujte Klientskou linku České spořitelny na bezplatném telefonním čísle 800 207 207.

Při používaní klientského certifikátu v internetovém bankovnictví také nenechávejte vaši čipovou kartu s klientským certifikátem ve čtečce čipových karet, jestliže neprovádíte bankovní operace, ale používejte ji pouze pro přihlášení a autorizaci transakcí. Pokud pro autorizaci transakcí používáte SMS zprávy, pečlivě čtěte jejich znění před vložením autorizačního kódu k transakci v internetovém bankovnictví.

Pokud budete dodržovat tyto zásady bezpečného používání internetbankingu, minimalizujete tak možnost zneužití vašich finančních prostředků. Další rady a tipy ohledně bezpečnosti najdete na www.csas.cz/bezpecnost.

Česká spořitelna

Obrázek č. 5: Upozornění České spořitelny na nový počítačový vir. Dostupné na: http://www.csas.cz/banka/content/inet/internet/cs/news_ie_1983.xml (79).

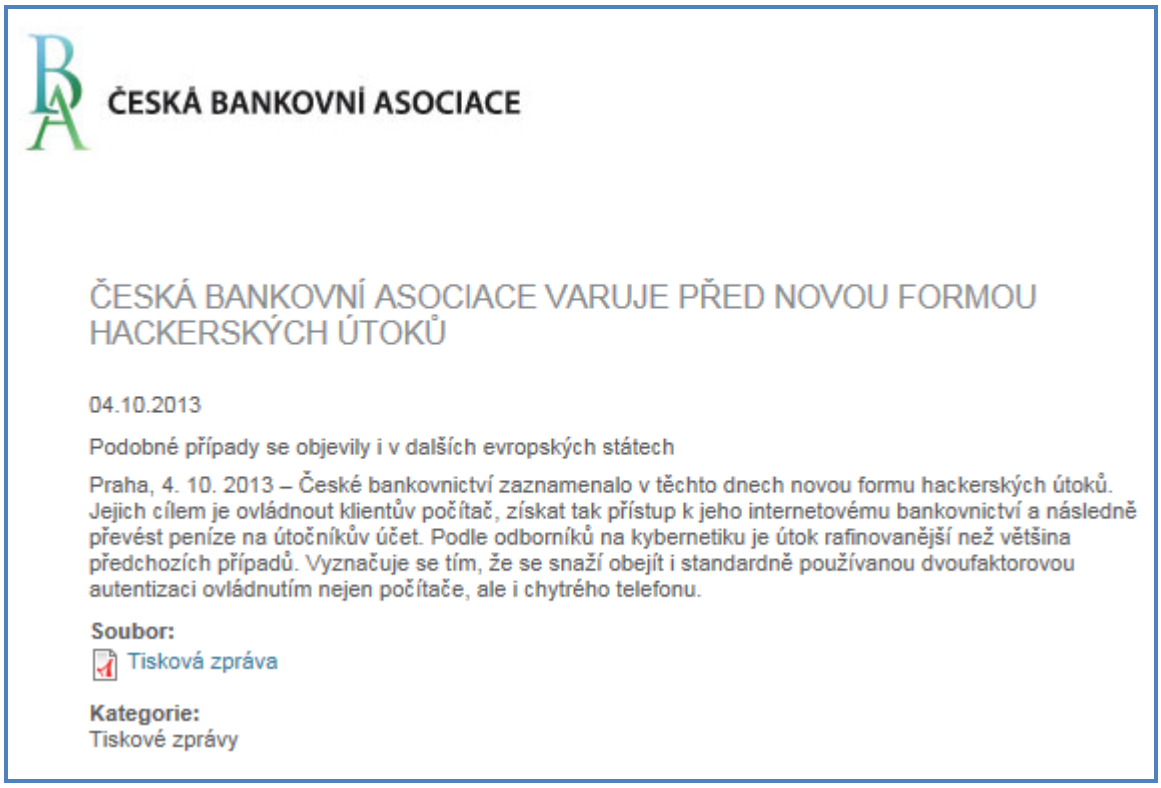
Na tomto příkladu je patrné, že **spolupráce** mezi subjekty mající zodpovědnost za určitou problematiku **není** vůbec dobře **nastavená**. Plánuje-li se v měsíci říjnu 2013, v tzv. evropském dni kybernetické bezpečnosti, prohloubení komunikace a spolupráce mezi zainteresovanými subjekty a navázání spolupráce s novými (informace na webu NCKB), můžeme předpokládat, že např. finanční a bankovní instituce, na které jsou podnikány časté útoky a zejména proti všem uživatelům využívající internetové bankovnictví, že reakce bezpečnostního týmu, do které oblast bankovnictví spadá, bude v minimálním stupni informovanosti rychlejší a úspěšnější. V Německu operuje bezpečnostní tým pouze pro sektor bankovních institucí,

v Rakousku síť mezi státním a soukromým sektorem, kde dochází k výměně aktuálních hrozeb a v České republice tým, který přináší aktuální informaci 17 dní po jejím zveřejnění na webu dotčené instituce. Bohužel, všude je psáno, že koordinace a spolupráce je nastavena (nad)standardně, uzavírají se smlouvy a memoranda, kterým ale chybí celkem zásadní aspekt – zodpovědnost a vyvození důsledků. Phishingové zprávy zneužívající uživatele České spořitelny, jsou podle veřejně dostupných informací nejčastějšími typy útoků. Jedná se o celosvětový fenomén, kdy se útočníci snaží získat přístupové údaje k bankovnímu účtu oběti (uživatele) takového útoku (68).

Česká pošta, s. p. zaznamenala pátý phishingový útok (viz Obrázek č. 6). Jako státní podnik, ale s komerčními aktivitami spadá jeho infrastruktura na národní CSIRT. V takovémhle případě i všech dalších by se nemělo hledět, kam který druh útoku spadá, respektive kdo má být týmem reakce – včetně upozornění, ale jedná-li se o vyšší počet uživatelů, což lze v tomto případu předpokládat, nemůže docházet k reakcím resp. nezveřejnění upozornění (77).

Obrázek č. 6: Varování České pošty před phishingovým útokem. Dostupné na: http://www.ceskaposta.cz/cz/aktualne/aktuality/2013/ceska-posta-zaznamenala-paty-phishingovy-utok-id41989 (77).

Varování **České bankovní asociace** (viz Obrázek č. 7) před novou formou hackerských útoků ze dne 4.10.2013 viz tisková zpráva (75; 76).



Obrázek č. 7: Varování České bankovní asociace. Dostupné na: https://www.czech-ba.cz/sites/default/files/dokumentyclanku/ceska-bankovni-asociace-varuje-pred-novou-formou-hackerskych-utoku/04102013tzcbaceskabankovniasociacevarujeprednovouformouhackerskychutokufinal.pdf (75).

Český vládní GovCERT ani národní CSIRT o informaci zatím **neinformovaly** (viz Obrázky č. 8, 9 ze dne 5.10.2013).

Obrázek č. 8: Žádné upozornění se na webu GovCERT neobjevilo. Dostupné na: http://www.govcert.cz/cs/informacni-servis/zranitelnosti (191).

Obrázek č. 9: Žádné upozornění se na webu CSIRT.CZ neobjevilo. Dostupné na: http://www.csirt.cz/news/security (69).

Předchozí reálné příklady poukazují na **špatně nastavenou spolupráci** v oblasti zveřejňování a sdílení informací vztahující se k bezpečnosti českého internetu. Určitě by neměl být problém, aby např. na stránkách národního týmu byla databáze, s omezeným přístupem (několika desítek jedinců v rámci České republiky) a podmínkou schválení ze strany určitého gestora týmu, ještě před zveřejněním (právě přidaných) aktuálních hrozeb různých subjektů, přednostně z ostatních bezpečnostních týmů České republiky, bankovního sektoru, poskytovateli internetových služeb, a těmi, kteří zásadním způsobem internet jako takový využívají a potřebují k existenci. Podle frekvence v současnosti takto zveřejňovaných zpráv (např. Česká spořitelna za měsíce srpen až září 2013 upozorňovala na tři incidenty spojené s podvodnými emaily a SMS zprávami) by se jednalo o zatím několik desítek zpráv za rok. V případě rozsáhlejšího útoku jako v březnu 2013 se i tak počet zveřejněných informací

vládního i národního týmu dostal na dvě zprávy CSIRT a tři zprávy NBÚ včetně několika vyjádření zástupců těchto institucí v médiích (78).

„Rekapitulace (D)DOS útoků ze dnů 4. 3. – 7. 3.“ je název dokumentu v odkazu uvádějící chybné datum – rok 2012, což si asi běžný uživatel nevšimne a na samotný dokument to nemá žádný vliv. V samotném dokumentu (obsahově pozitivním ke všem zúčastněným subjektům) jsou potvrzeny negativní zkušenosti při sdílení relevantních informací o útocích mezi přímo zúčastněnými subjekty, odkazující se na zákon a vyhlášky. Tímto je bráněno efektivní spolupráci mezi poskytovateli internetových služeb a bezpečnostními týmy (65).

V záložce Zajímavé odkazy je nefunkční odkaz (222), použijeme-li domovskou stránku **TERENA** (221) zjistíme, že „ti“ v uvedeném odkazu patří TERENA’s Trusted Introducer tzn., akreditační systém, který pomáhá budovat síť důvěry („Web of Trust“ pojem známý v rakouském CIRCA, viz kapitola 3.3) mezi bezpečnostními týmy CSIRT. Taková spolupráce musí být založena na silné **důvěře** mezi bezpečnostními týmy mnoha sektorů, zejména výzkumných, vzdělávacích, komerčních a státních institucí (218).

Výše popisované, svým způsobem pro mnoho čtenářů nevýznamné chyby na webu českého národního bezpečnostního týmu, však vyvolávají určité pochybnosti hraničící s **nedůvěrou**.

Aktivní spolupráce českých bezpečnostních týmů proběhla v březnu 2013 při tzv. (D)DoS útocích proti mediálním a finančním institucím České republiky. **Active24-CSIRT** analyzoval malware, **CESNET-CERTS** analyzoval provoz sítě CESNET2, CSIRT-MU monitoroval chování sítě Masarykovy univerzity a detekoval stopy vedoucí k podezření na malware, **CZ.NIC-CSIRT** se připravoval na možnost napadení autoritativních DNS (Domain Name Server) serverů v doméně .cz a webových služeb, **CSIRT.CZ** komunikoval s ostatními **CSIRT** týmy a subjekty, shromažďoval, vyhodnocoval a distribuoval informace, byl v kontaktu s dalšími potenciálními cíli útoku, zajišťoval komunikaci s médii, byl v kontaktu s NBÚ a bezpečnostními složkami (160).

Některé **prvky spolupráce** proběhly téměř podle části „Strategie pro oblast kybernetické bezpečnosti České republiky na období 2012 – 2015“ kde se zdůrazňuje žádoucí koordinace všech iniciativ, ať už státních, komerčních a akademických subjektů, a kde pouze spojené úsilí má vést k posílení kybernetické bezpečnosti a nebude docházet ke tříštění sil a mnohdy zbytečnému dublování činností. Vzájemná důvěra a sdílení informací jsou základním předpokladem pro **úspěšnou vzájemnou spolupráci** mezi veřejným a soukromým sektorem (186).

Cílené DDoS útoky proti webům zpravodajských, finančních a bankovních institucí. Webové stránky iDNES.cz, iHNED.cz, Novinky.cz, Lidovky.cz, Deník.cz, Živě.cz, Mobilmania.cz a E15.cz byly dne 4.3.2012 pod rozsáhlými DDoS útoky. Následujícího dne útoky pokračovaly proti webu Seznam.cz a dne 6.3.2013 proti službám (internetové bankovnictví, terminálové platby, atd.) České národní banky, České spořitelny, ČSOB, Fio banky, KB, Pražské burzy cenných papírů, Raiffeisenbank. Informace o provedených útocích potvrdili provozovatelé dotčených webů. Vyšetřování útoků zatím poukazuje na přístupy zejména z ruských a českých IP adres. Situace je nadále analyzována i ze strany NBÚ, CZ.NIC, CESNET, BIS a jiných subjektů (83).

Vyjádření výkonného ředitele sdružení **CZ.NIC** ke kybernetickým útokům v České republice. Ředitel CZ.NIC se vyjádřil (12.3.2013) k nedávným útokům na české weby. Pravděpodobně se nejednalo o útok typu DDoS, ale jen DoS (Denial of Service) a je možné, že se na jeho tvorbě nepodílel placený botnet, ale jen cíleně sestavený systém. Ačkoli útok nebyl nijak složitý, dokázal vyřadit z provozu například i platební terminály nebo SMS služby, což svědčí o špatné struktuře a zabezpečení českých poskytovatelů služeb. Řada stop ukazuje, že útok měl původ v ruské síti **RETN**, ale ruská strana zatím neposkytla podrobnější informace. Během vyšetřování se také projevilo nedostatečné legislativní podchycení kybernetické bezpečnosti, které například komplikuje sdílení informací o provozu na síti (73; 243).

Návrh **zákona o kybernetické bezpečnosti** byl po meziresortním připomínkovém řízení zaslán dne 28.6.2013 vládě ČR k projednání[7] (176; 177). Důvodová zpráva viz odkaz (175).

Samotný návrh **„Zákona o kybernetické bezpečnosti“** počítá s postupem „Varování“ (viz § 14) který zatím, podle dosavadních zkušeností (viz předchozí), vázne na vzájemné spolupráci mezi subjekty (podle Zákona národní CERT nebo orgány, vykonávající působnost v oblasti kybernetické bezpečnosti v zahraničí). Varování má zveřejnit NBÚ (v zákoně jako Úřad) na webu vládního CERT a dále je oznámí povinným osobám podle Zákona (viz § 3). Na počátku této kapitoly prezentované reálné zkušenosti s opožděnými resp. nezveřejněnými hrozbami (předpokládejme nevelkého rozsahu nesouvisející se stavem kybernetického nebezpečí, viz § 14) prostřednictvím národního CSIRT zatím nenasvědčují správně nastavené koordinaci a spolupráci mezi vládním a národním týmem, kde by tak podle návrhu Zákona mělo být. V rámci prevence by jakákoli varování měla být zveřejňována na vládním i národním webu. Do doby účinnosti zákona (je předpokládáno datum 1.1.2015) je zatím ještě časový prostor tyto a případně jiné navrhované postupy nastavit i účinně. V současnosti (říjen 2013) tomu tak není. Několikrát zde zmiňovaná **důvěra** resp. nedůvěra je bohužel i na straně Zákona (Varování viz výše), dále to, že správní delikty projednává samotný Úřad (nezahájí-li řízení do jednoho roku resp. tří let od spáchání správního deliktu, odpovědnost právnické osoby zaniká; právnická osoba nenese odpovědnost, prokáže-li, že vynaložila veškeré úsilí vedoucí k zabránění porušení právní povinnosti – Kdo posoudí pojem veškeré úsilí?); výše deliktů v rozmezí od deseti tisíc do sta tisíc korun českých (viz § 30, pro některé komerční subjekty téměř směšné částky, pro některé možná i likvidační). NBÚ nedisponuje vlastními zaměstnanci z řad počítačových odborníků, kteří by byli schopni posuzovat některá stanovená kritéria. Bude docházet k posudkům ze strany soukromých subjektů nebo postačí zákonná úprava, kterou zpracovával NBÚ a vystačí si s tím? Objevují se i názory (viz Nápravník, 2013), že by Zákon neměl stát samostatně, ale měl by být součástí zákona o krizovém řízení (248), kde jsou informační a komunikační systémy odvětvovými kritérii kritické

[7] 2.1.2014 byl Návrh zákona o kybernetické bezpečnosti schválen vládou České republiky viz http://www.nbu.cz/cs/aktuality/1262-vlada-2-ledna-2014-schvalila-navrh-zakona-o-kyberneticke-bezpecnosti nebo http://www.vlada.cz/cz/media-centrum/tiskove-zpravy/vysledky-jednani-vlady--2--ledna-2014-114800.

infrastruktury. Zůstává nepřehledná, pro někoho možná i chaotická posloupnost subjektů, **NBÚ** (jako národní autorita problematiky – sídlo v Praze), **NCKB** (zbytečný mezistupeň, sídlo v Brně), **vládní CERT** (GovCERT, spadající pod NCKB), **národní CSIRT** (provozovaný sdružením CZ.NIC – správcem české národní domény, sídlo v Praze). Český kybernetický prostor a právní prostředí „Zákona o kybernetické bezpečnosti“ čeká zatěžkávací zkouška nedaleké a reálné budoucnosti.

„Zpráva o činnosti CSIRT.CZ (Národního CSIRT ČR) za rok 2012“ vydaná 10.5.2013 viz odkaz (64). Český vládní GovCERT.cz podobnou zprávu zatím nevydal.

Výkladový slovník kybernetické bezpečnosti – druhé vydání. „Policejní akademie ČR a Česká pobočka AFCEA za aktivní podpory pracovníků NBÚ ČR, Národního centra kybernetické bezpečnosti a odborné veřejnosti vydaly druhé, rozšířené vydání slovníku kybernetické bezpečnosti doplněné o anglický překlad českého výkladu odborných výrazů.“ (153; 189).

Projekt **„Czech CyberCrime Centre of Excellence“** tzv. C4E, je realizován Masarykovou univerzitou v Brně ve spolupráci s několika subjekty státní i komerční sféry (např. NBÚ, Kriminalistický ústav Praha, Risk Analysis Consultants s.r.o.) za finanční podpory Evropské unie. Hlavním cílem projektu je vytvoření kvalitního centra pro školení a vzdělávání v oblasti prevence a represe kybernetické kriminality. Období projektu je v rozsahu května 2013 do dubna 2015.[8]

[8] Detail projektu viz https://www.muni.cz/ics/research/projects/23963?lang=cs.

5. Zhodnocení výsledků a doporučení

Kapitola hodnotí výsledky analytické části.

Spolupráce CERTs států Evropské unie je s určitostí na postupném rozvoji aktivit vedoucí k prohlubování výše zmiňované důvěry (dříve jako Web of Trust). V rámci Evropy je nejaktivnějším subjektem posledních let agentura ENISA. V rámci jednotlivých států patří mezi nejaktivnější Nizozemí – sídla institutů Terena, Europol (EC3) a Estonsko, jako vůdčí země Evropské unie v oblasti kybernetické bezpečnosti.

Porovnáním přínosu informací zveřejňovaných na oficiálních stránkách některých týmů CERT se najdou i značné rozdíly. Český vládní CERT uveřejňuje (říjen 2013) na svých stránkách (191) jednou za 14 dní jednu informaci (minimálně se vztahující k České republice) zejména o zranitelnostech produktů, chybách v zabezpečení, případně bezpečnostních aktualizacích. Přínos pro čtenáře je **minimální**. Zprávy ztrácejí svoji hodnotu ze dne na den někdy i z hodiny na hodinu. Má-li čtenář zájem o informace téměř v reálném čase, může si vybrat z několika nabídek, které jsou svým přínosem na daleko vyšší úrovni, alespoň co se rozmanitosti a frekvence zpráv týče. V rámci Evropy určitě **CERT-EU**, který uvádí každou hodinu několik zpráv z různých zdrojů, podobně je na tom britský portál NewsNow (198), který automaticky a průběžně (každých pět minut) aktualizuje titulky s odkazy na zpravodajské servery z celého světa. Odkazuje na něj i celosvětový CSIRT. Mimo Evropu a v trochu jiném formátu je materiál amerického **US-CERT** vycházející každý pracovní den „The DHS Daily Open Source Infrastructure Report“. Denní souhrn publikovaných informací z otevřených zdrojů týkající se významných kritických infrastruktur. Přehled je rozdělený na několik odvětví kritické infrastruktury a klíčových aktiv definovaných v „the National Infrastructure Protection Plan“ (81; 82).

Je až politování hodné, že český tým, který vznikl v rámci Evropské unie jako jeden z posledních vůbec, nedokázal využít mnohaleté zkušenosti jiných týmů. Přitom český národní CSIRT provozovaný sdružením CZ.NIC, který do doby zřízení vládního CERTu zastával

i jeho roli, a je v úzké spolupráci s NBÚ jako gestorem kybernetické bezpečnosti, má v současnosti (říjen 2013) na svých stránkách několika násobně vyšší produkci (říjen 2013) a to jak zkráceným českým překladem, tak i uveřejněním odkazu na původní zprávu. Určitě není problém, odkud a jaké typy zpráv zveřejňovat. Možnosti existují a jinými subjekty jsou využívány. Český čtenář má i přesto daleko větší možnosti na několika zahraničních portálech. Jiným typem formátu jsou blogy jako např. **CERT/CC** blog, kde jsou příspěvky bezpečnostních odborníků CERT zveřejňující vlastní zkušenosti. Příspěvky jsou zhruba jednou dvakrát týdně (oproti českému týmu několikanásobné) avšak obsahově velmi odborné (26). Podobné blogy mají i soukromé bezpečnostní společnosti jako např. AVG (12), Symantec (213), FireEye (132), Emsisoft (87), Kaspersky (154) a jiné, které jsou velmi odborné a velké množství společností (včetně vládních a národních týmů) jejich příspěvky pravidelně využívají ve svých rubrikách.

Z výše uvedených důvodů, lze **přínos českého CERTu** pro uživatele hledající alespoň základní informace k počítačové bezpečnosti hodnotit tou nejhorší možnou známkou. Z veřejně dostupných informací je známo, že provoz českého vládního CERTu stojí desítky milionů korun ročně a zatím jsou vidět minimální přínosy, které by ve výši jednoho procenta z ročního rozpočtu mohly být zásadní. Nabízí se, zde již několikrát opakované a svým způsobem nejcharakterističtější slovo – spolupráce, a to zejména s akademickou sférou jako nezbytným předpokladem dalšího úsilí. Základními výhodami takové spolupráce jsou především mezioboroví specialisté různých oborů, kteří dokážou plnit specifické úkoly v řadě akademických pracovišť, jejichž výsledky patří mezi světovou špičku a to za vynaložení mnohem nižších finančních prostředků. S tím souvisí i do budoucna problematická personální obsazenost, technická znalost, zajištění **důvěrné komunikace** s dalšími zúčastněnými subjekty vedoucí ke snadnější výměně relevantních a kvalitních informací, dohody, memoranda, průběžný vývoj důvěry.

6. Závěr

Diplomová práce je rozdělena do devíti kapitol, z toho kapitola třetí (teoretická) objasňuje historické souvislosti vzniku CERTs v USA, Asii a Evropě. Kapitola čtvrtá (analytická) je zaměřena na konkrétní výstupy jednotlivých CERTs, případně jiných subjektů a eventuálních rozdílností daných výstupů. Kapitola pátá hodnotí výsledky analytické části.

Hlavním cílem práce bylo porovnání působnosti národních týmů zejména členských států Evropské unie. Kapitola třetí shrnuje základní, teoretické informace této problematiky. Kapitola čtvrtá se zaměřuje na samotné, aktuální výstupy jednotlivých týmů a dalších subjektů včetně krátkého shrnutí dané zprávy.

Jako dílčí cíle byly stanoveny - vytvoření uceleného přehledu řešené problematiky a analýza současného stavu ve vybraných evropských státech. Toto je obsaženo zejména v kapitole číslo tři pro dané oblasti resp. státy. Dalším dílčím cílem byla analýza aktuálních hrozeb kybernetické bezpečnosti, které jsou zpracovány v kapitole číslo čtyři v názorných příkladech situačních zpráv a studiích vydaných společnostmi, které jsou úzce napojeny na státní případně nadnárodní instituce (národní CERTs, ENISA, Europol).

Hlavní metodou práce byla komparace a dokumentová analýza, která byla využita ke studiu a analýze odborných informačních zdrojů zejména v analytické části.

Existují tři dimenze aktivit na úrovni vládní, národní a mezinárodní. Spolupráce na mezinárodní úrovni je po administrativní stránce nastavena spolehlivě. Bohužel, v minulosti již uskutečněná kybernetická cvičení evropských týmů ukázala, že praxe je odlišná. Vládní a národní úroveň jednotlivých států je také rozdílná. V samotných státech, díky vymezeným reálným hranicím, je úroveň komunikace nastavena na vyšší úrovni, ale i zde se objevují rozdílnosti mezi státy. Neexistuje ideální řešení, v představách a na papíru zcela určitě, ale samotná realita již několikrát ukázala, že slova spolupráce, koordinace, zodpovědnost a důvěra jsou nejlepší cestou k přiblížení se představám.

Rozdílná řešení v rámci jednotlivých států vedou k duplicitnímu úsilí a řešení, v některých případech i k izolovanosti a nekoordinovanosti. Je velmi důležité odstranit duplicitní úkoly a činnosti, pokud existuje několik národních nebo vládních týmů CERT v jedné zemi. Nabízí se vícestranné dohody s externími subjekty zejména internetovými poskytovateli, mobilními operátory a příslušnými státními orgány na poli spolupráce a sdílení informací o kybernetických incidentech.

Samotné národní resp. vládní týmy nemohou být jedinou instancí k ochraně kybernetického prostoru daného státu. Nedílnou součástí jsou univerzitní týmy (centra) a komerční společnosti specializované na kybernetickou bezpečnost, usnadňující strategickou spolupráci a sdílení informací pro lepší identifikaci a koordinaci mezi zúčastněnými stranami s možností řešit národní i mezinárodní priority a problémy související s kyberprostorem. Týmy CERT by v rámci každého státu měly mít nastavené vlastní, odzkoušené procesy, které zaručují efektivní spolupráci s minimálními dopady na zájmové kritické informační struktury v případě ohrožení nebo nefunkčnosti z důvodu kybernetických útoků. Opakuje se již několikrát zde popisovaná a nezpochybnitelná, systematická a strategická spolupráce mezi státním, univerzitním a soukromým sektorem.

Velikost státu svou rozlohou neznamená větší počet týmů. Estonsko jako stát s nejrozšířenější digitální infrastrukturou a se zkušenostmi kybernetických útoků, má jeden oficiální CERT, stejně jako např. Slovensko a Slovinsko, Polsko čtyři, Rakousko pět, Česká republika šest, Německo 22. Počet týmů v rámci jednoho státu není důležitý. Ukotvení rozsahu pravomocí jednotlivých týmů, koordinace, a zejména úzká spolupráce se subjekty různých odvětví může vést alespoň k částečné, v některých případech i kompletní ochraně kritických informačních infrastruktur. Bezpečnostní týmy CERT nejsou dokonalým řešením a nezaručují absolutní bezpečnost. Existence těchto týmů je jen jedním z aspektů oblasti počítačové bezpečnosti, které jsou účastni všichni, počínaje správci sítí a služeb, manažery, internetovými poskytovateli a provozovateli služeb, bezpečnostními složkami státu a státem samotným, a přinejmenším všech uživatelů, kteří by měli dodržovat a znát základní pravidla chování zejména na internetu.

7. Seznam použitých zdrojů

(1) ACTIVE 24, 2013: *ACTIVE24-CSIRT*. ACTIVE 24.
Dostupné na: http://www.active24.cz/csirt, cit. 4.6.2013.

(2) ACTIVE 24, 2013: *O nás.* ACTIVE 24.
Dostupné na: http://www.active24.cz/o-spolecnosti/o-spolecnosti-active24, cit. 4.6.2013.

(3) AFCEA, 2013: *Home*. Česká pobočka AFCEA.
Dostupné na: http://www.afcea.cz, cit. 4.6.2013.

(4) AFCEA, 2013: *Kdo jsme*. Česká pobočka AFCEA.
Dostupné na: http://www.afcea.cz/obsah/kdo-jsme, cit. 4.6.2013.

(5) AllThingsD, 2013: *Microsoft and Google Will Sue U.S. Government Over FISA Order Data*. Dow Jones & Company. Dostupné na: http://allthingsd.com/20130830/microsoft-and-google-will-sue-u-s-government-over-fisa-order-data. cit. 8.9.2013.

(6) APCERT, 2013: *About APCERT*. Asia Pacific CERT.
Dostupné na: http://www.apcert.org/about/index.html, cit. 1.6.2013.

(7) APCERT, 2003: *Annual Report*. Asia Pacific CERT. Dostupné na:
http://www.apcert.org/documents/pdf/annualreport2003.pdf, cit. 1.6.2013.

(8) APCERT, 2013: *Mission Statement*. Asia Pacific CERT.
Dostupné na: http://www.apcert.org/about/mission/index.html, cit. 1.6.2013.

(9) APWG, 2013: *About the APWG*. Anti-Phishing Working Group.
Dostupné na: http://www.antiphishing.org/about-APWG, cit. 20.7.2013.

(10) Arbor Networks, 2010: *Attack Severs Burma Internet*. Arbor Networks. Dostupné na:
http://asert.arbornetworks.com/2010/11/attac-severs-myanmar-internet, cit. 2.9.2013.

(11) ASPI, 2013: *Special Report - The emerging agenda for cybersecurity*. Australian Strategic Policy Institute. Dostupné na:
http://www.aspi.org.au/publications/publication_details.aspx?ContentID=369&pubtype=-1, cit. 1.8.2013.

(12) AVG, 2013: *AVG Blogs*. AVG Technologies.
Dostupné na: http://blogs.avg.com, cit. 20.10.2013.

(13) BBC, 2013: *Global internet slows after 'biggest attack in history'*. BBC. Dostupné na:
http://www.bbc.co.uk/news/technology-21954636, cit. 24.8.2013.

(14) Bürger-CERT, 2013: *Über uns*. BSI.
Dostupné na: https://www.buerger-cert.de/about, cit. 7.6.2013.

(15) CBS, 2013: *Intelligence chief offers dire warning on cyberattacks*. CBC Interactive.
Dostupné na:
http://news.cnet.com/8301-1009_3-57573902-83/intelligence-chief-offers-dire-warning-on-cyberattacks. cit. 15.6.2013.

(16) CCDCOE, 2013: *CCD COE login*. NATO CCD COE.
Dostupné na: https://portal.ccdcoe.org, cit. 3.6.2013.

(17) CCDCOE, 2013: *Cyber Defence*. NATO CCD COE.
Dostupné na: http://www.ccdcoe.org/2.html, cit. 3.6.2013.

(18) CCDCOE, 2010: *Frameworks for International Cyber Security*. NATO CCD COE.
Dostupné na: http://www.ccdcoe.org/publications/books/FICS1.pdf, cit. 20.8.2013.

(19) CCDCOE, 2010: *Frameworks for International Cyber Security – International Case Law*. NATO CCD COE. Dostupné na: http://www.ccdcoe.org/publications/books/FICS2.pdf, cit. 22.9.2013.

(20) CCDCOE, 2012: *National Cyber Security Framework Manual*. NATO CCD COE.
Dostupné na: http://ccdcoe.org/369.html, cit. 18.8.2013.

(21) CCDCOE, 2012: *National Strategies & Policies*. NATO CCD COE.
Dostupné na: http://www.ccdcoe.org/328.html, cit. 25.9.2013.

(22) CCDCOE, 2013: *New Cyber Security Status Watch Report Available*. NATO CCD COE.
Dostupné na: http://www.ccdcoe.org/434.html, cit. 3.6.2013.

(23) CCDCOE, 2013: *Press announcement of the CCDCOE.* NATO CCD COE.
Dostupné na: http://ccdcoe.org/21.html, cit. 3.6.2013.

(24) CCDCOE, 2012: *The Tallinn Manual*. NATO CCD COE.
Dostupné na: http://www.ccdcoe.org/249.html, 1.5.2013.

(25) CEC, 2006: *A Strategy for a Secure Information Society – "Dialogue, partnership and empowerment"*. Commission of the European Communities. Dostupné na:
http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0251en01.pdf, cit. 4.7.2013.

(26) CERT, 2013: *CERT Blogs*. Carnegie Mellon University.
Dostupné na: http://www.cert.org/blogs, cit. 20.10.2013.

(27) CERT-EU, 2013: *About Us*. CERT-EU.
Dostupné na: http://cert.europa.eu/cert/plainedition/en/cert_about.html, cit. 6.6.2013.

(28) CERT-EU, 2013: *Latest News About – Ongoing threats*. CERT-EU.
Dostupné na: http://cert.europa.eu, cit. 4.7.2013.

(29) CERT-EU, 2013: *RFC 2350*. CERT-EU.
Dostupné na: http://cert.europa.eu/static/RFC2350/RFC2350.pdf, cit. 6.6.2013.

(30) CERT-EU, 2013: *Security White Papers*. CERT-EU. Dostupné na:
http://cert.europa.eu/cert/newsletter/en/latest_Publications%20and%20Newsletters_.html,
cit. 4.7.2013.

(31) CERT-EU, 2013: *Top Stories*. CERT-EU. Dostupné na:
http://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html , cit. 4.7.2013.

(32) CERT-Bund, 2013: *RFC-2350*. BSI. Dostupné na:
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Kritis/rfc2350_CERT-
Bund_txt.txt?__blob=publicationFile, cit. 7.6.2013.

(33) CERT-Bund, 2013*: Über CERT-Bund*. BSI.
Dostupné na: https://www.cert-bund.de/about, cit. 7.6.2013.

(34) CERT-EE, 2013: *About*. CERT-EE. Dostupné na: http://www.cert.ee, cit. 3.6.2013.

(35) CERT-EE, 2013: *RFC 2350 Description for CERT-EE*. CERT-EE.
Dostupné na: http://www.cert.ee/cert-ee-rfc2350.txt, 3.6.2013.

(36) CERT-Verbund, 2013: *Übersicht*. DFN-CERT.
Dostupné na: http://www.cert-verbund.de, cit. 7.6.2013.

(37) CERT.at, 2010: *Bericht Internet-Sicherheit Österreich 2010*. CERT.at. Dostupné na:
http://www.cert.at/static/downloads/reports/cert.at-jahresbericht-2010.pdf, cit. 7.6.2013

(38) CERT.at, 2013: *Blog*. Computer Emergency Response Team Austria.
Dostupné na: http://www.cert.at/services/blog/ListPage1_en.html, cit. 24.8.2013.

(39) CERT.at, 2013: *Circa*. Computer Emergency Response Team Austria.
Dostupné na: http://www.cert.at/about/circa/content.html, cit. 7.6.2013.

(40) CERT.at, 2013: *Overview*. Computer Emergency Response Team Austria.
Dostupné na: http://www.cert.at/index_en.html, 7.6.2013.

(41) CERT.at, 2013: *RFC 2350*. Computer Emergency Response Team Austria.
Dostupné na: http://www.cert.at/about/rfc2350/rfc2350_en.html, 7.6.2013.

(42) CERT.at, 2013: *Software*. Computer Emergency Response Team Austria.
Dostupné na: http://www.cert.at/downloads/software/ListPage1_en.html,cit. 24.8.2013.

(43) CERT Estonia, 2012: *Information about cyber attacks in Georgia, sent by CERT Estonia experts from Georgia*. EISA. Dostupné na: https://www.ria.ee/information-about-cyber-attacks-in-georgia-sent-by-cert-estonia-experts-from-georgia, cit. 2.9.2013.

(44) CERT Estonia, 2012: *Malicious cyber attacks against Estonia come from abroad*. EISA. Dostupné na: https://www.ria.ee/malicious-cyber-attacks-against-estonia-come-from-abroad, cit. 2.9.2013.

(45) CERT Estonia, 2010: *Digital Agenda: cyber-security experts test defences in first pan-European simulation.* EISA. Dostupné na:
https://www.ria.ee/digital-agenda-cyber-security-experts-test-defences-in-first-pan-european-simulation, cit. 8.7.2013.

(46) CERT Estonia, 2013: *About CERT Estonia*. EISA.
Dostupné na: https://www.ria.ee/cert-estonia, 3.6.2013.

(47) CERT Estonia, 2013: *Facts about e-Estonia.* EISA.
Dostupné na: https://www.ria.ee/facts-about-e-estonia, 3.6.2013.

(48) CERT Polska, 2013: *Informacje*. NASK. Dostupné na: http://www.cert.pl, cit. 7.6.2013.

(49) CERT Polska, 2013: *Informacje*. NASK.
Dostupné na: http://www.cert.pl/langswitch_lang/en, cit. 7.6.2013.

(50) CERT Polska, 2013: *ZeuS-P2P monitoring and analysis*. CERT Polska.
Dostupné na: http://www.cert.pl/PDF/2013-06-p2p-rap_en.pdf, cit. 23.8.2013.

(51) CSIRT, 2013: *CSIRT Incident Response Teams*. CSIRT.
Dostupné na: http://www.csirt.org/irt_teams/index.html, cit. 4.6.2013.

(52) CSIRT, 2013: *HyperRFC*. CSIRT.
Dostupné na: http://www.csirt.org/rfc_csirt/doc/rfc2350.txt, cit. 4.6.2013.

(53) CSIRT, 2013: *Request for Comments*. CSIRT.
Dostupné na: http://www.csirt.org/rfc_csirt/index.html, cit. 4.6.2013.

(54) CSIRT.CZ, 2013: *O nás*. CZ.NIC.
Dostupné na: http://www.csirt.cz/page/882/o-nas, cit. 4.6.2013.

(55) CSIRT.SK, 2013: *Prehľad voľne dostupných antivírusových riešení.* CSIRT.SK. Dostupné na: http://www.csirt.gov.sk/informacna-bezpecnost/virusove-infiltracie/volne-dostupne-av-81a.html, cit. 7.6.2013.

(56) CIRC, 2013: *Úvod*. Centrum CIRC. Dostupné na: http://circ.army.cz, cit. 4.6.2013.

(57) CESNET, 2013: *O nás*. CESNET. Dostupné na: http://www.cesnet.cz/sdruzeni, cit. 4.6.2013.

(58) CESNET, 2013: *Síť CESNET2*. CESNET. Dostupné na: http://www.cesnet.cz/sluzby/pripojeni/sit-cesnet2, cit. 4.6.2013.

(59) CESNET-CERTS, 2013: *O nás*. CESNET. Dostupné na: https://csirt.cesnet.cz, cit. 4.6.2013.

(60) CNCERT/CC, 2013: *About Us*. The National CERT Center of China. Dostupné na: http://www.cert.org.cn/publish/english/index.html, cit. 1.6.2013.

(61) CNCERT/CC, JPCERT/CC and KrCERT/CC, 2013: *The First China-Japan-Korea CSIRT Annual Meeting for Cybersecurity Incident Response.* The National CERT Center of China. Dostupné na: http://www.cert.org.cn/publish/english/upload/File/The%20First%20CJK%20Annual%20Meeting%20for%20Cybersecurity%20Incident%20Response_Press%20Release.pdf, cit. 1.6.2013.

(62) CSIRT.CZ, 2013: *RFC 2350*. CZ.NIC. Dostupné na: http://www.csirt.cz/files/csirt/rfc2350_CSIRT.CZ.20130323.pdf, cit 4.6.2013.

(63) CSIRT.CZ, 2013: *Novinky*. CZ.NIC. Dostupné na: http://www.csirt.cz, cit. 1.10.2013.

(64) CSIRT.CZ, 2013: *Zpráva o činnosti CSIRT.CZ*. CZ.NIC. Dostupné na: http://www.csirt.cz/files/csirt/Zprava_o_cinnosti_CSIRT.CZ.2012.pdf, cit. 25.5.2013.

(65) CSIRT.CZ, 2013: *Rekapitulace (D)DOS útoků ze dnů 4. 3. – 7. 3.* CZ.NIC. Dostupné na: http://www.csirt.cz/files/csirt/Rekapitulace-utoky-20120311.pdf, cit. 5.10.2013.

(66) CSIRT.CZ, 2013*: Novinky.* CZ.NIC. Dostupné na: http://www.csirt.cz, cit. 4.6.2013.

(67) CSIRT.CZ, 2013: *Memoranda*. CZ.NIC. Dostupné na: http://www.csirt.cz/files/csirt/Memorandum_nbu.pdf, cit. 4.6.2013.

(68) CSIRT.CZ, 2013: *CSIRT.CZ zachytil phishingovou zprávu směřující na uživatele České spořitelny.* CZ.NIC. Dostupné na: http://csirt.cz/page/1633/csirt.cz-zachytil-phishingovou-zpravu-smerujici-na-uzivatele-ceske-sporitelny, cit. 1.10.2013.

(69) CSIRT.CZ, 2013: *Aktuálně z bezpečnosti*. CZ.NIC.
Dostupné na: http://www.csirt.cz/news/security, cit. 5.10.2013.

(70) CSIRT.SK, 2013: *Harmonogram vytvorenia CSIRT.SK*. CSIRT.SK.
Dostupné na: http://www.csirt.gov.sk/doc/CSIRT.SK.pdf, cit. 7.6.2013.

(71) CSIRT.SK, 2013: *RFC 2350*. CSIRT.SK.
Dostupné na: http://www.csirt.gov.sk/o-nas/rfc-2350-7e7.html, cit. 7.6.2013.

(72) CSIRT.SK, 2013: *Vitajte!* CSIRT.SK. Dostupné na: http://www.csirt.gov.sk, cit. 7.6.2013.

(73) CZ.NIC blog, 2013: *DDoS nebo DoS? Aneb jak se dá udělat útok*. CZ.NIC. Dostupné na: http://blog.nic.cz/2013/03/11/ddos-nebo-dos-aneb-jak-se-da-udelat-utok, cit. 11.3.2013.

(74) CyberSecurity, 2013: *Exkurz do kybernetické bezpečnosti.* CyberSecurity.
Dostupné na: http://www.cybersecurity.cz/data/kb120404.pdf, cit. 5.6.2013.

(75) ČBA, 2013: *Česká bankovní asociace varuje před novou formou hackerských útoků*. Česká bankovní asociace. Dostupné na: https://www.czech-ba.cz/sites/default/files/dokumentyclanku/ceska-bankovni-asociace-varuje-pred-novou-formou-hackerskych-utoku/04102013tzcbaceskabankovniasociacevarujeprednovouformouhackerskychutokufinal.pdf, cit. 5.10.2013

(76) ČBA, 2013: *Home*. Česká bankovní asociace.
Dostupné na: https://www.czech-ba.cz, cit. 5.10.2013.

(77) Česká pošta, 2013: *Česká pošta zaznamenala pátý phishingový útok*. Česká pošta. Dostupné na: http://www.ceskaposta.cz/cz/aktualne/aktuality/2013/ceska-posta-zaznamenala-paty-phishingovy-utok-id41989, cit. 3.10.2013

(78) Česká spořitelna, 2013: *Aktuality*. Česká spořitelna. Dostupné na: http://www.csas.cz/banka/appmanager/portal/banka?_nfpb=true&_pageLabel=news_archive_subportal03, cit. 5.10.2013.

(79) Česká spořitelna, 2013: *Aktuality*. Česká spořitelna. Dostupné na: http://www.csas.cz/banka/content/inet/internet/cs/news_ie_1983.xml, cit. 4.9.2013.

(80) ČSN ISO 27032 (369790). *Informační technologie - Bezpečnostní techniky - Směrnice pro kybernetickou bezpečnost*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

(81) DHS, 2013: *The DHS Daily Open Source Infrastructure Report*. The Department of Homeland Security. Dostupné na: http://www.dhs.gov/dhs-daily-open-source-infrastructure-report, cit. 20.10.2013.

(82) DHS, 2013: *The National Infrastructure Protection Plan*. The Department of Homeland Security. Dostupné na: http://www.dhs.gov/national-infrastructure-protection-plan, cit. 20.10.2013.

(83) Dočekal, Vyleťal, Slížek., 2013: *Weby českých bank ochromil DDoS útok, NBÚ žádá od postižených data.* Lupa.cz. Dostupné na: http://www.lupa.cz/clanky/web-ceske-sporitelny-neni-dostupny-vcetne-sluzeb-servis24, cit. 6.3.2013.

(84) eArchiv.cz, 2011: *Archiv článků a přednášek Jiřího Peterky*. Jiří Peterka. Dostupné na: http://www.earchiv.cz/b04/b1109001.php3, cit. 27.5.2013.

(85) EGC group, 2013: *Contacts.* EGC. Dostupné na: http://www.egc-group.org/contact.html, cit. 10.6.2013.

(86) EGC group, 2013: *European Government CERTs Group*. EGC. Dostupné na: http://www.egc-group.org, cit. 10.6.2013.

(87) Emsisoft, 2013: *Blog.Emsisoft.Com*. Emsisoft. Dostupné na. http://blog.emsisoft.com, cit. 20.10.2013.

(88) ENISA, 2009: *Emergency Response to Security Breaches*. ENISA. Dostupné na: http://www.enisa.europa.eu/activities/cert/background/files/CERTS_April_2008_hires.pdf, cit. 7.7.2013.

(89) ENISA, 2010: *Cyber Europe 2010*. ENISA. Dostupné na: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/ce2010, cit. 7.7.2013.

(90) ENISA, 2011: *6th CERT workshop (past)*. ENISA. Dostupné na: http://www.enisa.europa.eu/activities/cert/events/6th-workshop-cybercrime, cit. 9.7.2013

(91) ENISA, 2012: *Cyber Europe 2012*. ENISA. Dostupné na: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/cyber-europe-2012, cit. 7.7.2013.

(92) ENISA, 2012: *Cyber Europe 2012 - Key Findings Report*. ENISA. Dostupné na: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/cyber-europe-2012/cyber-europe-2012-key-findings-report, cit. 7.7.2013.

(93) ENISA, 2012: *Cyber Incident Reporting in the EU*. ENISA. Dostupné na: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu , cit. 8.7.2013.

(94) ENISA, 2012: *First International Conference Cyber Crisis Cooperation: Cyber Exercises.* ENISA. Dostupné na: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/conference/cyber-exercise-conference, cit. 6.7.2013.

(95) ENISA, 2012*: Proactive detection of security incidents II - Honeypots*. ENISA. Dostupné na: http://www.enisa.europa.eu/activities/cert/support/proactive-detection-of-security-incidents-II-honeypots, cit. 8.7.2013.

(96) ENISA, 2012: *Status report 2012*. ENISA. Dostupné na: http://www.enisa.europa.eu/activities/cert/support/files/status-report-2012, cit. 5.7.2013.

(97) ENISA, 2013: *8th CERT workshop – Part I.* ENISA. Dostupné na: http://www.enisa.europa.eu/activities/cert/events/8th-cert-workshop-part-I, cit. 9.7.2013.

(98) ENISA, 2013: *8th CERT workshop – Part II.* ENISA. Dostupné na: http://www.enisa.europa.eu/activities/cert/events/8th-cert-workshop-part-ii, cit. 9.7.2013.

(99) ENISA, 2013: *Andrea Dufkova*. ENISA. Dostupné na: http://www.enisa.europa.eu/activities/cert/contact/andrea-dufkova, cit. 4.6.2013.

(100) ENISA, 2013: *Annual Incident Reports 2012*. ENISA. Dostupné na: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2012 , cit. 7.7.2013.

(101) ENISA, 2013: *CERT*. ENISA. Dostupné na: http://www.enisa.europa.eu/activities/cert, cit. 6.6.2013.

(102) ENISA, 2013: *CERT factsheet*. ENISA. Dostupné na: http://www.enisa.europa.eu/activities/cert/background/cert-factsheet, cit. 6.6.2013.

(103) ENISA, 2013: *CERTs by Country – Interactive Map*. ENISA. Dostupné na: http://www.enisa.europa.eu/activities/cert/background/inv/certs-by-country-interactive-map cit. 8.6.2013.

(104) ENISA, 2013: *Cyber Security Strategy of the Czech Republic for the 2011-2015 Period*. ENISA. Dostupné na: http://www.enisa.europa.eu/media/news-items/CZ_Cyber_Security_Strategy_20112015.PDF, cit. 4.6.2013.

(105) ENISA, 2013: *ENISA Threat Landscape mid year 2013*. ENISA. Dostupné na: http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-mid-year-2013, cit. 7.7.2013.

(106) ENISA, 2013: *European Cyber Security Month*. ENISA. Dostupné na: http://cybersecuritymonth.eu, cit. 1.10.2013.

(107) ENISA, 2013*: European Cyber Security Month – Czech Republic*. ENISA. Dostupné na: http://cybersecuritymonth.eu/ecsm-countries/czech-republic, cit. 1.10.2013.

(108) ENISA, 2013: *European Union Agency for Network and Information Security*. ENISA. Dostupné na: http://www.enisa.europa.eu, cit. 6.6.2013.

(109) ENISA, 2013: Flash *Note: Can Recent Attacks Really Threaten Internet Availability?* ENISA. Dostupné na: http://www.enisa.europa.eu/publications/flash-notes/flash-note-can-recent-attacks-really-threaten-internet-availability, cit. 6.7.2013

(110) ENISA, 2013: *Flash note: Cyber-attacks – a new edge for old weapons*. ENISA. Dostupné na: http://www.enisa.europa.eu/publications/flash-notes/cyber-attacks-2013-a-new-edge-for-old-weapons, cit. 6.7.2013.

(111) ENISA, 2013*: Inventory of CERT activities in Europe*. ENISA. Dostupné na: http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe , cit. 4.6.2013.

(112) ENISA, 2013: *Inventory of CERT activities in Europe*. ENISA. Dostupné na: http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe , cit. 4.6.2013.

(113) ENISA, 2013: *National Cyber Security Strategies: An Implementation Guide*. ENISA. Dostupné na: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide, cit. 5.7.2013.

(114) ENISA, 2013: *National-level Risk Assessments: An Analysis Report*. ENISA. Dostupné na: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/nlra-analysis-report, cit. 20.11.2013.

(115) ENISA, 2013: *Successful conclusion of 2nd International Conference on Cyber Crisis Cooperation & Exercises.* ENISA. Dostupné na: http://www.enisa.europa.eu/media/news-items/successful-conclusion-of-2nd-international-conference-on-cyber-crisis-cooperation-exercises, cit. 6.7.2013.

(116) ENISA, 2013: *What´s ECSM*. ENISA. Dostupné na: http://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/european-cyber-security-month-advocacy-campaign, cit. 1.10.2013.

(117) ESET, 2013: *Virus Radar.* Eset. Dostupné na: http://www.virusovyradar.sk, cit. 7.6.2013.

(118) EUR-Lex, 2009: *Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience.* European Union Law. Dostupné na: http://eur-lex.europa.eu/Notice.do?checktexts=checkbox&val=493232:cs&pos=1&page=1&lang=en&pgs=10&nbl=1&list=493232:cs,&hwords=&action=GO&visu , cit. 4.7.2013.

(119) European Commission, 2010: *A strategy for smart, sustainable and inclusive growth*. European Union Law. Dostupné na: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:EN:PDF, cit. 4.7.2013.

(120) European Commission, 2013: *EU Cybersecurity plan to protect open internet and Dostupné na freedom and opportunity - Cyber Security strategy and Proposal for a Directive*. Europa.eu. Dostupné na: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-Dostupné na-freedom-and-opportunity-cyber-security , cit. 4.7.2013.

(121) European Commission, 2013: *Press releases database*. Europa.eu. Dostupné na: http://europa.eu/rapid/press-release_IP-13-94_en.htm, cit. 4.7.2013.

(122) European Commission, 2013: *Questions and Answers: Directive on attacks against information systems*. Europa.eu.
Dostupné na: http://europa.eu/rapid/press-release_MEMO-13-661_en.htm, cit. 9.7.2013.

(123) European Parliament, 2013: *Cyber attacks: Parliament adopts stricter EU-wide penalties*. Europa.eu. Dostupné na: http://www.europarl.europa.eu/news/en/pressroom/content/20130701IPR14763/html/Cyber-attacks-Parliament-adopts-stricter-EU-wide-penalties, cit. 9.7.2013.

(124) European Parliament, 2013: *Defending against cyber attacks*. European Parliament. Dostupné na: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede251010audnatocyberattacks_/sede251010audnatocyberattacks_en.pdf, cit. 4.6.2013.

(125) Europol, 2013: *A Collective EU Response to Cybercrime*. Europol.
Dostupné na: https://www.europol.europa.eu/ec3, cit. 20.7.2013.

(126) Europol, 2013*: Cybercrime: A Growing Global Problem*. Europol.
Dostupné na: https://www.europol.europa.eu/ec/cybercrime-growing, cit. 3.6.2013.

(127) Europol, 2013: *EC3 Advisory Groups*. Europol.
Dostupné na: https://www.europol.europa.eu/ec3/ec3-advisory-groups, cit. 3.6.2013.

(128) Europol, 2013: *Europol-Interpol Cybercrime Conference 2013*. Europol. Dostupné na: https://www.europol.europa.eu/content/europol-interpol-cybercrime-conference-2013, cit. 25.8.2013.

(129) Europol, 2013: *Europol and Interpol Chiefs Review Trends in International Policing*. Europol. Dostupné na:
https://www.europol.europa.eu/content/europol-and-interpol-chiefs-review-trends-international-policing, cit. 25.8.2013.

(130) Europol, 2013: *Europol SOCTA 2013*. Europol. Dostupné na:
https://www.europol.europa.eu/sites/default/files/publications/europol_socta_2013_report.pdf, cit. 25.8.2013.

(131) FBI, 2013: *IC3 2012 Internet Crime Report Released*. FBI.gov. Dostupné na:
http://www.fbi.gov/news/pressrel/press-releases/ic3-2012-internet-crime-report-released, cit. 13.6.2013.

(132) FireEye, 2013*: Blog*. FireEye. Dostupné na: http://www.fireeye.com/blog, 20.10.2013.

(133) FIRST, 2013: *About FIRST*. FIRST.org. Dostupné na: http://www.first.org/about, cit. 27.5.2013.

(134) FIRST, 2013: *Forum for Incident Response and Security Teams*. FIRST.org.
Dostupné na: http://www.first.org , cit. 27.5.2013.

(135) FNR, 2013: *FBI launches iGuardian to standardize cyber threat data sharing*. Federal News Radio. Dostupné na: http://www.federalnewsradio.com/490/3406415/FBI-launches-iGuardian-to-standardize-cyber-threat-data-sharing, cit. 1.8.2013.

(136) GovCERT.AT, 2013: *Austrian GovCERT.* Govcert.gv.at.
Dostupné na: http://www.govcert.gv.at/index_en.html, cit. 7.6.2013.

(137) GovCERT.AT, 2013: *Internationale Kooperationen*. Govcert.gv.at.
Dostupné na: http://www.govcert.gv.at/home/cooperation/content.html, cit. 7.6.2013.

(138) GovCERT.AT, 2013: *Links und Dokumente*. Govcert.gv.at.
Dostupné na: http://www.govcert.gv.at/home/links/content.html, cit. 7.6.2013.

(139) GovCERT.AT, 2013: *Nationale Aufgaben*. Govcert.gv.at.
Dostupné na: http://www.govcert.gv.at/home/scope/content.html, cit 7.6.2013.

(140) GOV.UK, 2013: *Digital Britain, digital India, digital world*. Crown Copyright. Dostupné na:
https://www.gov.uk/government/speeches/digital-britain-digital-india-digital-world,
cit. 26.9.2013.

(141) GOV.UK, 2013: *Establishing a Cyber Security Information Sharihg Partnership*. Crown Copyright. Dostupné na:
https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace/supporting-pages/establishing-a-cyber-security-information-sharing-partnership, cit. 26.9.2013.

(142) GOV.UK, 2013: *Setting up a National Cyber Crime Unit*. Crown Copyright. Dostupné na:
https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace/supporting-pages/setting-up-a-national-cyber-crime-unit, cit. 26.9.2013.

(143) HNS, 2013: *INTERPOL Chief on fighting cybercrime worldwide*. Help Net Security. Dostupné na: http://www.net-security.org/secworld.php?id=14745 , cit. 9.7.2013.

(144) IC3, 2012: *Internet Crime Report 2012*. Internet Crime Complaint Center.
Dostupné na: http://www.ic3.gov/media/annualreport/2012_IC3Report.pdf, cit. 13.6.2013.

(145) ICSPA, 2013: *Project 2020*. International Cyber Security Protection Alliance. Dostupné na: https://www.europol.europa.eu/sites/default/files/publications/2020_white_paper.pdf,
cit. 25.9.2013.

(146) InfraGard, 2013*: Washington D.C. InfraGard FAQ's*. InfraGard. Dostupné na:
https://www.infragard.org/SXrBmL%2525252B0cR92Tm4EVWYydCCff7B0N35IXPPcUXW8NrY%2525253D, cit. 1.8.2013.

(147) Interpol, 2013: *Europol-INTERPOL Cybercrime Conference 2013*. Interpol.
Dostupné na:
http://www.interpol.int/News-and-media/Events/2013/Europol-INTERPOL-Cybercrime-Conference-20132/Europol-INTERPOL-Cybercrime-Conference-2013, cit. 25.8.2013.

(148) Interpol, 2013: *Europol-INTERPOL Cybercrime Conference to enhance cooperation in protecting cyberspace.* Interpol. Dostupné na:
http://www.interpol.int/News-and-media/News-media-releases/2013/N20130925,
cit. 25.8.2013.

(149) ISCP, 2013: *Annual Report 2013-2013*. Intelligence and Security Committee of Parliament. Dostupné na: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/2012-2013_ISC_AR.pdf?attachauth=ANoY7crcmSGWl0O8JEEqDarjgVk2vi9CRAZ7VuGy9vuQxI5XdS5AkmvIH6IGAj0B18JFldiK5yYT8H3i8htuUpmKKGvEaflZaRTl-q4N65x2BVMyN1EmVsWl3GbIuDuYyCaaIxAlhWAksRAh073giKSWeA34LuaOV2iV3C9x4lECgK2-HGWUwuYzeTnvXifNwVjCX7R0_VKDSK2CAagWk-qWXAAmG9ABfLwD13X4mnBAEu02aj25L54%3D&attredirects=0, cit. 13.7.2013.

(150) IDG News Service, 2012: *EU cybersecurity agency says variation between countries adds risk*. IDG. Dostupné na: http://news.idg.no/cw/art.cfm?id=A53FC674-F373-BF23-01E8D8BE3084E9D2, cit. 9.7.2013.

(151) Interpol, 2013: *Kaspersky Lab to support INTERPOL Global Complex for Innovation with advanced tools and expertise*. Interpol. Dostupné na: http://www.interpol.int/News-and-media/News-media-releases/2013/PR037, cit. 9.7.2013.

(152) James R. Clapper, 2013: *Worldwide Threat Assessment of the US Intelligence Community.* Office of the Director of National Intelligence. Dostupné na: http://odni.gov/files/documents/Intelligence%20Reports/2013%20ATA%20SFR%20for%20SSCI%2012%20Mar%202013.pdf, cit. 15.6.2013.

(153) Jirásek, Novák, Požár, 2013: *Výkladový slovník kybernetické bezpečnosti.* Policejní akademie ČR & Česká pobočka AFCEA, 200 str.,
Dostupné na: http://www.govcert.cz/download/nodeid-561, cit. 22.6.2013.

(154) Kaspersky Lab, 2013: *Blog. Kaspersky Lab*.
Dostupné na: http://www.securelist.com/en/blog, cit. 20.10.2013.

(155) Kaspersky Lab, 2013: *The „Icefog" APT: A Tale of Cloak and Three Daggers*. Kaspersky Lab.
Dostupné na: http://www.securelist.com/en/downloads/vlpdfs/icefog.pdf, cit. 27.9.2013.

(156) Kaspersky Lab, 2013: *The Icefog APT: Frequently Asked Questions*. Kaspersky Lab.
Dostupné na: http://www.securelist.com/en/analysis/204792307/The_Icefog_APT_Frequently_Asked_Questions, cit. 27.9.2013.

(157) Katri Lindau, 2012: *Cyber Security in Estonia: Lessons from the Year 2007 Cyberattack*. Tallinn University.
Dostupné na: www.cs.tlu.ee/teemaderegister/get_file.php?id=195, cit. 2.9.2013.

(158) KPN, 2013: *Organisation*. KPN.
Dostupné na: http://www.kpn-cert.nl/en/organisatie.html, cit. 5.6.2013.

(159) KPN, 2013: *Welcome to KPN-CERT*. KPN.
Dostupné na: http://www.kpn-cert.nl/en/index.html, cit. 5.6.2013.

(160) Kropáčová A., 2013: *CERT/CSIRT týmy a jejich role*. Root.cz.
Dostupné na: http://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role, cit. 6.5.2013.

(161) Le Monde, 2013: *Révélations sur le Big Brother français*. Le Monde.
Dostupné na: http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html, cit. 5.7.2013.

(162) Microsoft, 2012: *Microsoft Reaches Settlement with Defendants in Nitol Case*. Microsoft Corporation. Dostupné na:
http://blogs.technet.com/b/microsoft_blog/archive/2012/10/02/microsoft-reaches-settlement-with-defendants-in-nitol-case.aspx, cit. 7.7.2013.

(163) Microsoft, 2013: *Microsoft works with financial services industry leaders, law enforcement and others to disrupt massive financial cybercrime ring*. Microsoft Corporation. Dostupné na:
http://blogs.technet.com/b/microsoft_blog/archive/2013/06/05/microsoft-works-with-financial-services-industry-leaders-law-enforcement-and-others-to-disrupt-massive-financial-cybercrime-ring.aspx, cit. 7.7.2013.

(164) MJG. *Cyber Espionage Against Georgian Government*. Ministry of Justice of Georgia.
Dostupné na: http://dea.gov.ge/uploads/CERT%20DOCS/Cyber%20Espionage.pdf,
cit. 2013-03-21.

(165) MU ÚVT, 2013: *O týmu*. Masarykova univerzita, Ústav výpočetní techniky.
Dostupné na: http://www.muni.cz/ics/services/csirt/about, cit. 4.6.2013.

(166) MU ÚVT, 2013: *Bezpečnostní tým CSIRT-MU*. Masarykova univerzita, Ústav výpočetní techniky. Dostupné na: http://www.muni.cz/ics/services/csirt, cit. 4.6.2013.

(167) NASK, 2013: *Aktualności*. NASK. Dostupné na: http://www.nask.pl, cit. 23.8.2013.

(168) NASK, 2013: *NASK shuts down dangerous Virut botnet domains*. NASK. Dostupné na:
http://www.cert.pl/news/6666/langswitch_lang/en, cit. 23.8.2013.

(169) NASK, 2013: *Posty*. NASK.
Dostupné na: http://www.cert.pl/langswitch_lang/pl, cit. 23.8.2013.

(170) NASK, 2013: *What´s new*. NASK.
Dostupné na: http://www.nask.pl/nask_en, cit. 23.8.2013.

(171) NASK, 2013: *Who we are*. NASK.
Dostupné na: ttp://www.nask.pl/run/n/Who_we_are, cit. 7.6.2013.

(172) NATO, 2013: *Defence Ministers make progress on cyber protection*. NATO. Dostupné na: http://www.nato.int/cps/en/SID-D32A3743-E7F29592/natolive/news_101143.htm, cit. 6.6.2013.

(173) NATO, 2013: *NATO and cyber defence*. NATO.
Dostupné na: http://www.nato.int/cps/en/natolive/topics_78170.htm, cit. 5.6.2013.

(174) Nápravník, Jiří, 2013: *Kyber-bezpečnost a připravovaný zákon*. Hospodářské noviny.
Dostupné na: http://napravnik.blog.ihned.cz/c1-59692700-kyber-bezpecnost-a-pripravovany-zakon, cit. 16.4.2013.

(175 NBÚ, 2013: *Důvodová zpráva k návrhu zákona o kybernetické bezpečnosti a o změně souvisejících zákonů*. Národní bezpečnostní úřad.
Dostupné na: http://www.nbu.cz/download/nodeid-1109, cit. 10.7.2013.

(176) NBÚ, 2013: *Návrh zákona o kybernetické bezpečnosti a o změně souvisejících zákonů*. Národní bezpečnostní úřad.
Dostupné na: http://www.nbu.cz/download/nodeid-1055, cit. 10.7.2013.

(177) NBÚ, 2013: *Návrh zákona o kybernetické bezpečnosti byl předložen vládě České republiky*. Národní bezpečnostní úřad. Dostupné na: http://www.nbu.cz/cs/aktuality/1398-navrh-zakona-o-kyberneticke-bezpecnosti-byl-predlozen-vlade-ceske-republiky, cit. 10.7.2013.

(178) NBÚ, 2013: *National Security Agency*. NBÚ.
Dostupné na: http://www.nbu.cz/en, cit. 4.6.2013.

(179) NCA, 2013: *About the NCA*. National Crime Agency.
Dostupné na: http://www.nationalcrimeagency.gov.uk, cit. 26.9.2013.

(180) NCBI, 2013: *Aktuální informace o odborných konferencích*. Národní centrum bezpečnějšího internetu. Dostupné na: http://konference.ncbi.cz, cit. 1.10.2013.

(181) NCBI, 2013: *Evropský měsíc kybernetické bezpečnosti*. Národní centrum bezpečnějšího internetu. Dostupné na: http://www.saferinternet.cz/ecsm-2013/ecsm-2013.html, cit. 1.10.2013.

(182) NCBI, 2013: *Konference Praha bezpečně online 2013*. Národní centrum bezpečnějšího internetu. Dostupné na: http://konference.ncbi.cz/konference-praha-bol-2013/konference-praha-bezpecne-online-2013.html, cit. 1.10.2013.

(183) NCBI, 2013: *Safer internet*. Národní centrum bezpečnějšího internetu. Dostupné na: http://www.saferinternet.cz, cit. 1.10.2013.

(184) NCIRC, 2013: *The NCIRC Technical Centre's Mission*. NCIRC.
Dostupné na: http://www.ncirc.nato.int, cit. 5.6.2013.

(185) NCKB, 2013: *Co je NCKB*. NBÚ. Dostupné na: http://www.govcert.cz/cs, cit. 4.6.2013.

(186) NCKB, 2013: *Další dokumenty*. NBÚ.
Dostupné na: http://www.govcert.cz/cs/legislativa/dalsi-dokumenty, cit. 5.6.2013.

(187) NCKB, 2013: *Doporučení pro případ napadení DDoS útokem - jak se zachovat a jak postupovat*. NBÚ. Dostupné na:
http://www.govcert.cz/cs/informacni-servis/aktuality/doporuceni-pro-pripad-napadeni-ddos-utokem---jak-se-zachovat-a-jak-postupovat, cit. 17.10.2013.

(188) NCKB, 2013: *Evropský měsíc kybernetické bezpečnosti*. NBÚ. Dostupné na:
http://www.govcert.cz/cs/informacni-servis/aktuality/evropsky-mesic-kyberneticke-bezpecnosti, cit. 1.10.2013.

(189) NCKB, 2013: *Výkladový slovník kybernetické bezpečnosti - druhé vydání*. NBÚ.
Dostupné na: http://www.govcert.cz/cs/informacni-servis/aktuality/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani, cit. 25.5.2013.

(190) NCKB, 2013: *Smlouvy a memoranda*. NBÚ.
Dostupné na: http://www.govcert.cz/download/nodeid-4727, cit. 4.6.2013.

(191) NCKB, 2013: Zranitelnosti. NBÚ,
Dostupné na: http://www.govcert.cz/cs/informacni-servis/zranitelnosti, cit. 5.10.2013.

(192) NCKB, 2013: *Zranitelnosti*. NBÚ. Dostupné na:
http://www.govcert.cz/cs/informacni-servis/zranitelnosti, cit. 20.10.2013.

(193) NCSC, 2013: *GOVCERT.NL*. NCSC. Dostupné na:
https://www.ncsc.nl/english/organisation/about-the-ncsc/govcert.nl.html, cit. 5.6.2013.

(194) NCSC, 2013: *DDOS attack caused disruption of the availability of websites.* National Cyber Security Center. Dostupné na:
https://www.ncsc.nl/english/current-topics/news/ddos-attack-caused-disruption-of-the-availability-of-websites.html, cit. 20.4.2013.

(195) NCSC, 2013: *Home.* NCSC. Dostupné na: https://www.ncsc.nl, cit. 5.6.2013.

(196) NCSC, 2013: *Home.* NCSC. Dostupné na: https://www.ncsc.nl/english, cit. 5.6.2013.

(197) NCSC, 2013: *International*. NCSC. Dostupné na:
https://www.ncsc.nl/english/organisation/partners/international.html, cit. 5.6.2013.

(198) NewsNow, 2013: *News.* NewsNow Publishing Limited.
Dostupné na: http://www.newsnow.co.uk/h, cit. 20.10.2013.

(199) Network World, 2010: *The WikiLeaks drama: A timeline*. Network World. Dostupné na: http://www.networkworld.com/news/2010/120910-the-wikileaks-drama-a.html, cit. 2.9.2013.

(200) Pro Publica, 2013: *Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security*. Pro Publica. Dostupné na: http://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption, cit. 7.9.2013.

(201) Phys.org, 2013: *Cyberattack deprives millions of Dutch of Dostupné na ID*. Phys.org. Dostupné na: http://phys.org/news/2013-04-cyberattack-deprives-millions-dutch, cit. 25.5.2013.

(202) Phys.org, 2013: *Cyberwar is reality world must fight: UN official*. Phys.org. Dostupné na: http://phys.org/news/2013-07-cyberwar-reality-world.html, cit. 16.7.2013.

(203) Reuters, 2013: *Microsoft says it freed millions of computers from criminal botnet*. Thomson Reuters. Dostupné na: http://www.reuters.com/article/2013/06/18/citadel-botnet-idUSL2N0EU22U20130618?type=companyNews, cit. 7.7.2013.

(204) Romania-Insider, 2013: *MiniDuke cyber attack could be state sponsored, greater impact than Red October*. Romania-Insider.com. Dostupné na: http://www.romania-insider.com/romanian-intelligence-service-miniduke-cyber-attack-could-be-state-sponsored-greater-impact-than-red-october/76553, cit. 5.4.2013.

(205) Shaun Tandon, 2013: *Obama says China hears 'blunt' message on hacking*. AFP. Dostupné na: http://www.google.com/hostednews/afp/article/ALeqM5ia2BD3J9QzFIR9AG4Vzl0QwPw2Rw?docId=CNG.16e6c69b7be76f5a169cef077ddfc721.4e1, cit. 18.7.2013.

(206) SiliconIndia News, 2013: *India To Have Cyber Security Policy Soon: Sibal.* SiliconIndia. Dostupné na: http://www.siliconindia.com/news/technology/India-To-Have-Cyber-Security-Policy-Soon-Sibal-nid-142158-cid-2.html, cit. 1.3.2013.

(207) Spamhaus, 2013: *About Spamhaus*. The Spamhaus Project.
Dostupné na: http://www.spamhaus.org/organization, cit. 24.8.2013.

(208) Spamhaus, 2013: *Spamhaus News Index*. The Spamhaus Project. Dostupné na: http://www.spamhaus.org/news/article/694/ddos-update-20-march-2013, cit. 24.8.2013.

(209) STO, 2013: *STO Events.* Science and Technology Organization.
Dostupné na: http://www.cso.nato.int, cit. 5.6.2013.

(210) SURF, 2013: *Teams*. SURF. Dostupné na:
http://www.surfnet.nl/nl/Thema/surfcert/teams/Pages/Default.aspx, cit. 5.6.2013.

(211) Symantec, 2013: *Hidden Lynx and MSS protection*. Symantec. Dostupné na:
http://www.symantec.com/connect/blogs/hidden-lynx-and-mss-protection, cit. 20.9.2013.

(212) Symantec, 2013: *Hidden Lynx – Professional Hackers for Hire*. Symantec. Dostupné na:
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/hidden_lynx.pdf, cit. 3.10.2013.

(213) Symantec, 2013: *Security Blogs*. Symantec.
Dostupné na: http://www.symantec.com/connect/security/blogs, cit. 20.10.2013.

(214) Symantec, 2013: *Snapshot of Virut Botnet After Interruption*. Symantec. Dostupné na:
http://www.symantec.com/connect/blogs/snapshot-virut-botnet-after-interruption,
cit. 23.8.2013.

(215) TERENA, 2013: *About TERENA*. TERENA.
Dostupné na: http://www.terena.org/about, cit. 10.6.2013.

(216) TERENA, 2013: *National Members*. TERENA.
Dostupné na: http://www.terena.org/about/people/ga.php, cit. 10.6.2013.

(217) TERENA, 2013: *TERENA National Members*. TERENA.
Dostupné na: http://www.terena.org/about/members_nat.php, cit. 10.6.2013.

(218) TERENA, 2011: *TERENA News*. TERENA. Dostupné na: http://www.terena.org
http://www.terena.org/news/fullstory.php?news_id=2925, cit. 6.10.2013.

(219) TERENA, 2013: *TF-CSIRT*. TERENA.
Dostupné na: http://www.terena.org/activities/tf-csirt, cit. 10.6.2013.

(220) TERENA, 2013: *TF-CSIRT/TI Restructuring Proposal*. TERENA. Dostupné na:
http://www.terena.org/activities/tf-csirt/publications/restructuring.pdf, cit. 10.6.2013.

(221) TERENA, 2013: *Welcome to TERENA*. TERENA. Dostupné na: http://www.terena.org,
cit. 6.10.2013.

(222) TERENA, 2013: *Welcome to TERENA*. TERENA. Dostupné na: http://www.ti.terena.nl,
cit. 6.10.2013.

(223) TF-CSIRT, 2013: *Services for Security and Incident Response Teams*. Trusted Introducer. Dostupné na: http://trusted-introducer.org, cit. 10.6.2013.

(224) TF-CSIRT, 2013: *Services for Security and Incident Response Teams*. Trusted Introducer. Dostupné na: http://www.trusted-introducer.nl, cit. 10.6.2013.

(225) The CERT Coordination Center, 2013: *About Us*. Carnegie Mellon University. Dostupné na: http://www.cert.org/meet_cert, cit. 26.5.2013.

(226) The CERT Coordination Center, 2013: *CERT*. Carnegie Mellon University. Dostupné na: http://www.cert.org/certcc.html, cit. 26.5.2013.

(227) The Journal of International Security, 2013: *The Digital Battlefield.* Intersec. Dostupné na: http://www.intersecmag.co.uk/article.php?id=42, cit. 9.7.2013.

(228) The Register, 2010: *DDoS attacks take out Asian nation*. The Register. Dostupné na: http://www.theregister.co.uk/2010/11/03/myanmar_ddos_attacks, cit. 2.9.2013.

(229) The Register, 2010: *Wikileaks outs 400,000 classified Iraq War docs*. The Register. Dostupné na: http://www.theregister.co.uk/2010/10/23/wikileaks_releases_four_hundred_thousand_iraq_war_docs, cit. 2.9.2013.

(230) The Guardian, 2013: *Barack Obama agrees to talks with Germany to explain spying on allies.* Guardian News. Dostupné na: http://www.guardian.co.uk/world/2013/jul/04/obama-agrees-talks-germany-spying, cit. 5.7.2013.

(231) The Guardian, 2013: *Revealed: how US and UK spy agencies defeat internet privacy and security.* Guardian News. Dostupné na: http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security, cit. 7.9.2013.

(232) The Guardian, 2013: *US and Germany to hold talks over European NSA surveillance concerns*. Guardian News. Dostupné na: http://www.guardian.co.uk/world/2013/jul/04/usa-germany-obama-merkel-talks-nsa, cit. 5.7.2013.

(233) The New York Times, 2013: *N.S.A. Able to Foil Basic Safeguards of Privacy on Web.* The New York Times Company. Dostupné na: http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?_r=0, cit. 7.9.2013.

(234) The Washington Post, 2013: *The NSA sponsors 'cyber operations' training at universities. Here's what students learn.* The Washington Post. Dostupné na: http://www.washingtonpost.com/blogs/the-switch/wp/2013/09/11/the-nsa-sponsors-cyber-operations-training-at-universities-heres-what-students-learn, cit. 20.9.2013.

(235) The Washington Times, 2013: *U.S.-Israeli cyberattack on Iran was 'act of force,' NATO study found.* The Washington Times. Dostupné na: http://www.washingtontimes.com/news/2013/mar/24/us-israeli-cyberattack-on-iran-was-act-of-force-na/?page=all#pagebreak, cit. 25.4.2013.

(236) The White House, 2012: *National Strategy for Information Sharing and Safeguarding*. Whitehouse.gov. Dostupné na: http://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf, cit. 15.6.2013.

(237) The White House, 2013: *FACT SHEET: U.S.-Russian Cooperation on Information and Communications Technology Security*. Whitehouse.gov. Dostupné na: http://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol, cit. 7.9.2013.

(238) Threatpost, 2013: *NSA's Alexander Appeals For Threat Information Sharing.* Threatpost. Dostupné na: http://threatpost.com/nsas-alexander-appeals-for-threat-information-sharing/102404, cit. 26.9.2013.

(239) US-CERT, 2013: *About Us*. The Department of Homeland Security. Dostupné na: http://www.us-cert.gov/about-us, cit. 26.5.2013.

(240) US-CERT, 2013: *NCCIC*. The Department of Homeland Security. Dostupné na: http://www.us-cert.gov/nccic, cit. 26.5.2013.

(241) U.S. Department of Defense, 2010: *Lynn: Cyberspace is the New Domain of Warfare*. U.S. Department of Defense. Dostupné na: http://www.defense.gov/News/NewsArticle.aspx?ID=61310, cit. 2.9.2013.

(242) U.S. Department of Defense, 2013: *The Cyber Domain.* The Department of Defense. Dostupné na: http://www.defense.gov/home/features/2013/0713_cyberdomain, cit. 26.5.2013.

(243) Vyleťal, Martin, 2013: *Ondřej Filip: Nečekejme, že při útoku přiběhnou chlapíci z CSIRTu a vše vyřeší.* Lupa.cz. Dostupné na: http://www.lupa.cz/clanky/ondrej-filip-necekejme-ze-pri-utoku-pribehnou-chlapici-z-csirtu-a-vse-vyresi, cit. 12.3.2013.

(244) WarDiaries, 2010: *Iraq & Afghan War Diaries Explorer.* Wikileaks.org. Dostupné na: http://warlogs.wikileaks.org, cit. 2.9.2013.

(245) Wired, 2010: *WikiLeaks' 400,000 Iraq War Documents Reveal Torture, Civilian Deaths*. Wired.com. Dostupné na: http://www.wired.com/threatlevel/2010/10/wikileaks-press, cit. 2.9.2013.

(246) WND, 2012: *Russian hackers beaten at their own game.* WND.com. Dostupné na: http://mobile.wnd.com/2012/11/russian-hackers-beaten-at-their-own-game, cit. 1.3.2013.

(247) Zákon o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů (Zákon č. 430/2010 Sb.). Dostupné na: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=72817&fulltext=&nr=430~2F2010&part=&name=&rpp=15#local-content, cit. 16.4.2013.

8. Seznam použitých zkratek

ACSC (Australian Cyber Security Centre)

AFCEA (Armed Forces Communications & Electronics Association)

APCERT (Asia Pacific Computer Emergency Response Team)

APT (Advanced Persistent Threat)

ASPI (Australian Strategic Policy Institute)

BKA (Bundeskanzleramt und Krisenmanagement)

BSI (Bundesamt für Sicherheit in der Informationstechnik

CCA (Consortium for Cybersecurity Action)

CERT (Computer Emergency Response Team)

CERT/CC (CERT Coordination Center)

CERT-Bund (Computer Emergency Response Team der Bundesverwaltung)

CERT-EE (The Computer Emergency Response Team of Estonia)

CERT-EU (Computer Emergency Response Team-European Union)

CESNET (Czech Education and Scientic Network)

CIIP (Critical Information Infrastructure Protection)

CIRC (Computer Incident Response Capability)

CIRCA (Computer Incident Response Coordination Austria)

CIRT (Computer Incident Response Team)

CISP (Cyber-security Information Sharing Partnership)

CSIRT (Computer Security Incident Response Team)

CSIRT-MU (Computer Security Incident Response Team of Masaryk University)

DDoS (Distributed Denial of Service)

DNS (Domain Name Server)

DoS (Denial of Service)

EARN (European Academic and Research Network)

ECSM (European Cyber Security Month)

EGC (The European Government CERTs group)

ENISA (European Network and Information Security Agency)

FIRST (Forum for Incident Response and Security Teams)

FISA (Foreign Intelligence Surveillance Act)

GCHQ (The Government Communications Headquarters)

GovCERT.AT (the Austrian Government Computer Emergency Response Team)

IC3 (Internet Crime Complaint Center)

ICS (The Intelligence and Security Committee)

IGCI (Interpol Global Complex for Innovation)

IP (Internet Protocol)

ISPA (Internet Service Providers Austria)

IT (Information Technology)

JVN (Japan Vulnerability Notes)

Myanmar MPT (The Myanma Posts and Telecommunications)

NASK (Research and Academic Computer Network

NATO CCD COE (Cooperative Cyber Defence Centre of Excellence)

NATO CIRC (Computer Incident Response Capability)

NBÚ (Národní bezpečnostní úřad)

NCA (National Crime Agency)

NCBI (Národní centrum bezpečnějšího internetu)

NCKB (Národní centrum kybernetické bezpečnosti)

NCSC (National Cyber Security Center)

NFC (Near Field Communication)

NSA (The National Security Agency)

RARE (Réseaux Associés pour la Recherche Européenne)

RFC (Request for Comments)

SOCA (the Serious Organised Crime Agency)

TERENA (Trans-European Research and Education Networking Association)

TF-CSIRT (The Task Force for Computer Security Incident Response Teams)

US-CERT (United States Computer Emergency Readiness Team)

USCYBERCOM (The United States Cyber Command)

9. Seznam obrázků

10. Seznam příloh

Příloha: Teze diplomové práce

Příloha: CD „Diplomová práce“