

Mgr. Klára Němečková, Mgr. Oldřich Krulík, Ph.D., doc. RNDr. Josef Požár, CSc., RNDr. Václav Hník, CSc.

Vývoj, související s budováním pracovišť typu CERT/CSIRT v České republice

Anotace

Ačkoli Česká republika patří mezi nejinternetizovanější země světa, její bezpečnostní politika v oblasti informačních a komunikačních technologií (ochrana kritické informační infrastruktury) za zbytkem Evropy spíše zaostává. Budování vrcholné hierarchie pracovišť typu CERT/CSIRT (ať už je nazveme vládní, národní či jinak) je nemyslitelné bez vkladu soukromého sektoru, který řadu funkcí státu v této oblasti supluje.

Klíčová slova

CERT/CSIRT, bezpečnostní politika v oblasti informačních a komunikačních technologií, ochrana kritické informační infrastruktury.

Annotation

Although the Czech Republic belongs among the most „internetised“ countries in the world, its information and communication security policy (as well as the protection of the critical information infrastructure) was lagged behind, when compared to the most of the rest European countries. Building of the hierarchy of the umbrella workplaces of the CERT/CSIRT type (regardless if we call them governmental, national or otherwise) is unthinkable without the contribution of private sector, who substitutes many functions of the state in this field.

Keywords

CERT/CSIRT, information and communication security policy, critical information infrastructure protection.

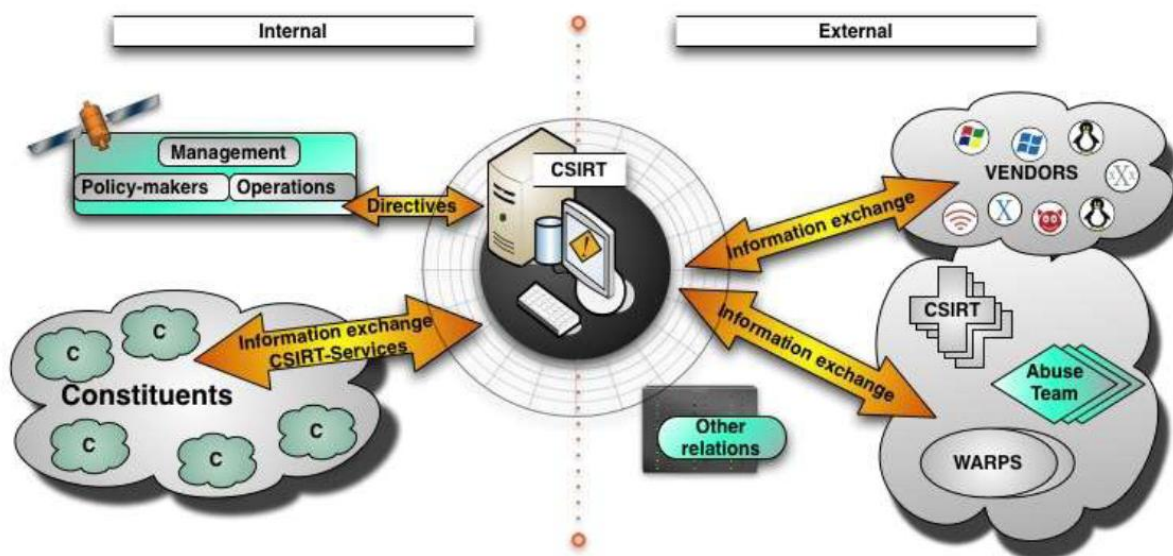
Pracoviště typu CERT/CSIRT a jejich význam

Nedílnou součástí preventivní a aktivní ochrany počítačů a počítačových sítí je důsledné a efektivní řešení bezpečnostních incidentů včetně odstraňování jejich příčin a následků. Je nutné, aby na možnost narušení bezpečnosti sítě a počítačů byli jejich správci a uživatelé připraveni a měli k dispozici funkční struktury, efektivní postupy, pravidla a technické prostředky vedoucí k co nejrychlejšímu odstranění problémů při minimalizaci škod.

Problematika zvládání incidentů tohoto charakteru je v řadě zemí světa řešena tzv. CERT týmy (Cybernetic Emergency Response Team, v češtině je užíván – například – překlad „hlásné středisko při kybernetických ohroženích“).¹

Služby nabízené CERT pracovištěm mohou zahrnovat služby *reaktivního* i *proaktivního* charakteru (školení, varování před aktuálními útoky, slabiny operačních systémů, bezpečnostní audity, konzultace ke konkrétnímu software, bezpečné konfigurace, vývoj a provoz nástrojů pro sledování provozu sítě a služeb a mnoho dalších aktivit).

Minimem je ovšem řešení bezpečnostních incidentů tak, aby byla naplněna myšlenka slova „response“ (tedy „odezva“ či „schopnost reagovat“), obsaženého ve zkratce CERT.²



Ilustrace: Pozice CERT pracoviště jako uzlového bodu v informační síti.

Zdroj: ENISA (European Network and Information Security Agency)

¹ Často užívaným synonymem tohoto pojmu je CSIRT (Cybernetic Security Incident Response Team), tedy „Tým pro odezvu při kybernetickém bezpečnostním incidentu“.

JIROVSKÝ, Václav; HNÍK, Václav; KRULÍK, Oldřich. Základní definice, vztahující se k tématu kybernetické bezpečnosti. Security Magazine. 2007, březen-duben, s. 46 až 49. ISSN 1210-8723.

² Ilustrace: <<http://www.enisa.europa.eu/activities/cert/support/guide2/external-relations/communities>>.

ENISA: CSIRT Communities <<http://www.zeably.com/csirt>>.

Vrcholový (národní, vládní) CERT v každé zemi představuje zachytný bod, na který se může uživatel (firma, občan, veřejná instituce) obrátit s konkrétním problémem, jehož řešení nezvládá vlastními silami. V případě kybernetického útoku ze zahraničí je komunikace mezi vrcholovými CERT týmy v jednotlivých zemích světa nezřídka rychlejší a efektivnější než kanály policejní spolupráce **(a je využitelná i při komunikaci se zeměmi, se kterými žádná policejní spolupráce nefunguje).**

Pracoviště typu CERT/CSIRT ve světě a v Evropě

Aktuální situace s ohledem na existenci pracovišť typu CERT/CSIRT v Evropě je následující:

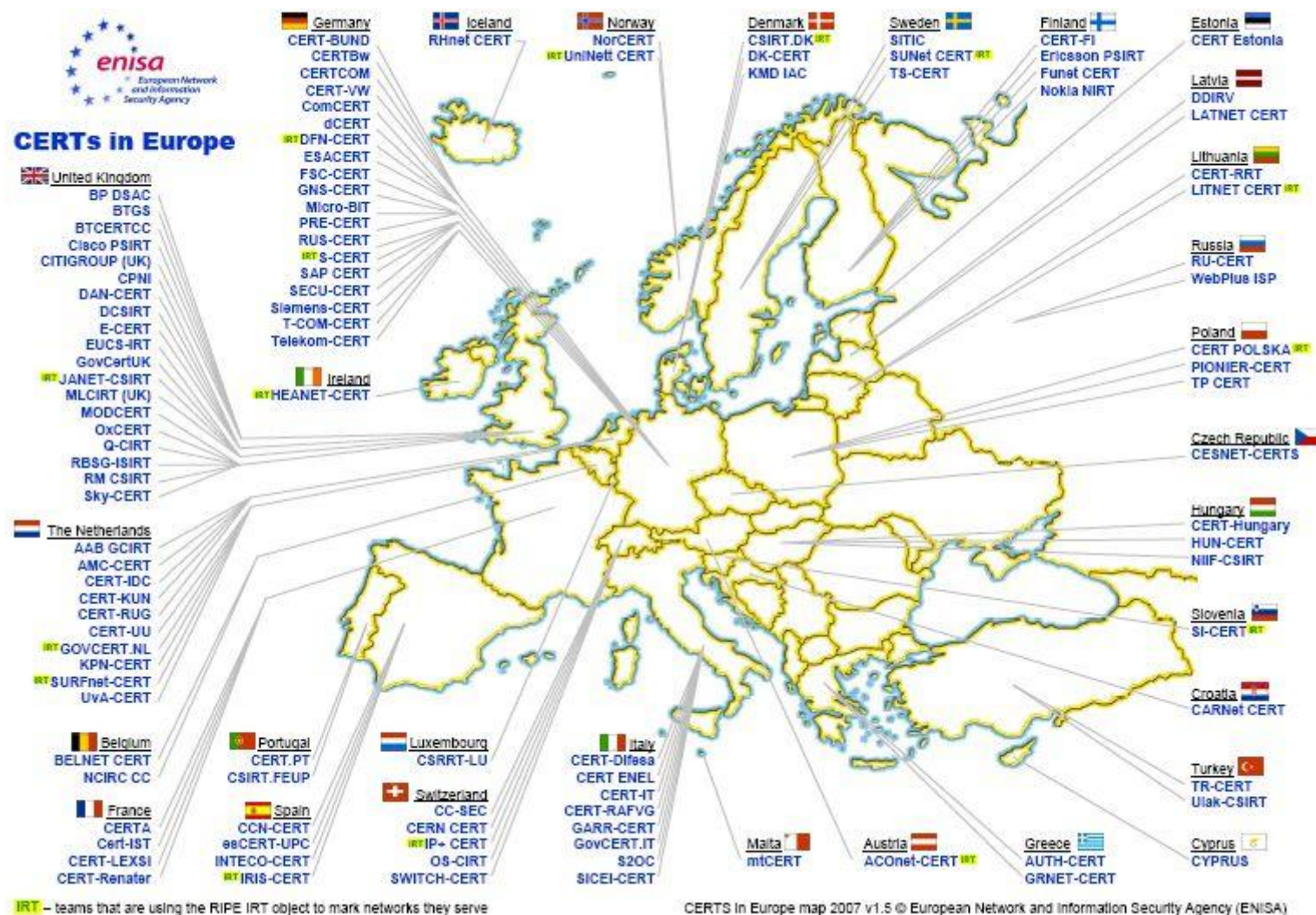
- „Alespoň nějaký“ CERT/CSIRT tým existuje v každém členském státu Evropské unie a v řadě dalších evropských zemích (v Ruské federaci, na Ukrajině, v Arménii, Moldávii, ve Švýcarsku, v Norsku, Srbsku či Chorvatsku).
- Některá vrcholová pracoviště jsou provozována nevládními (akademickými) subjekty (se slabší nebo silnější podporou státu). V jiných zemích provozují Národní pracoviště typu CERT pouze orgány státní správy.
- V řadě zemí existuje více či méně plnohodnotné „Národní pracoviště typu CERT/CSIRT“, sloužící nejširší veřejnosti nebo alespoň subjekty, které s větší nebo menší úspěšností roli národních CERT/CSIRT pracovišť "supluje" (mezi které patří i Česká republika, mimo Evropskou unii například Island³ atd.).
- V řadě zemí působí určitý počet omezenějších platforem typu CERT/CSIRT, zajišťujících servis pro konkrétní zákazníky.
- V některých zemích CERT/CSIRT tým slouží zejména vládním a vojenským strukturám (Turecko).
- V některých zemích tyto struktury vůbec neexistují (Bosna a Hercegovina, Makedonie, Albánie a Černá Hora).

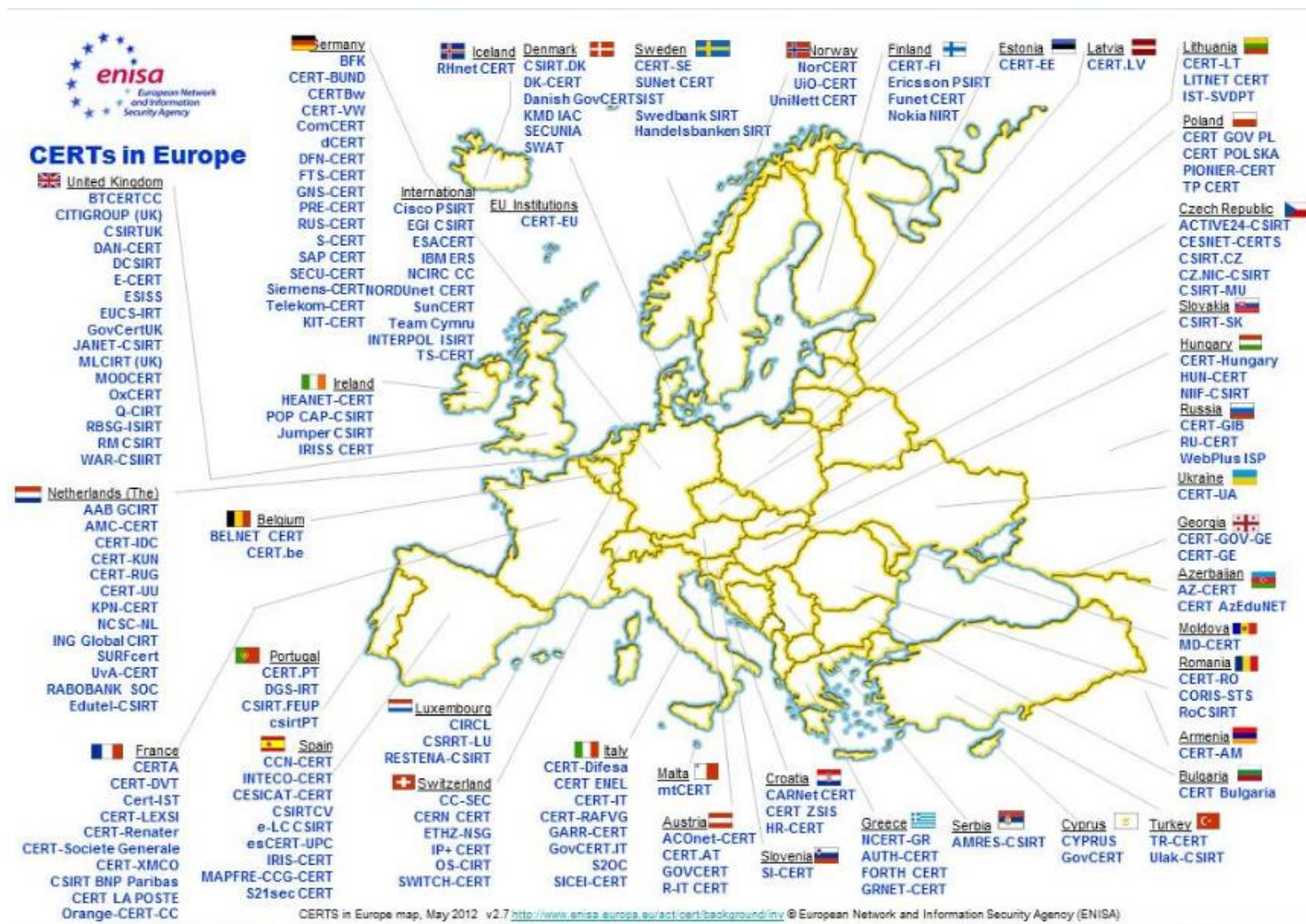
O „promořenosti“ současného světa respektive Evropy pracovišti typu CIRT/CSERT je možné si učinit představu z map Agentury ENISA (srovnání let 2007 a 2012: v České republice je roku 2007 uveden jen jeden subjekt – CESNET.CERTS, roku 2012 jich je už pět).⁴

³ HNÍK, Václav; KRULÍK, Oldřich; POŽÁR, Josef. Zajišťování informační bezpečnosti na Islandu jako inspirace pro Českou republiku. AFCEA, duben 2012. ISBN 978-80-7251-371-0 <<http://www.cybersecurity.cz/data/hnik.pdf>>; <<http://www.cybersecurity.cz/posts.html>>.

⁴ CERTs in Europe; in: ENISA

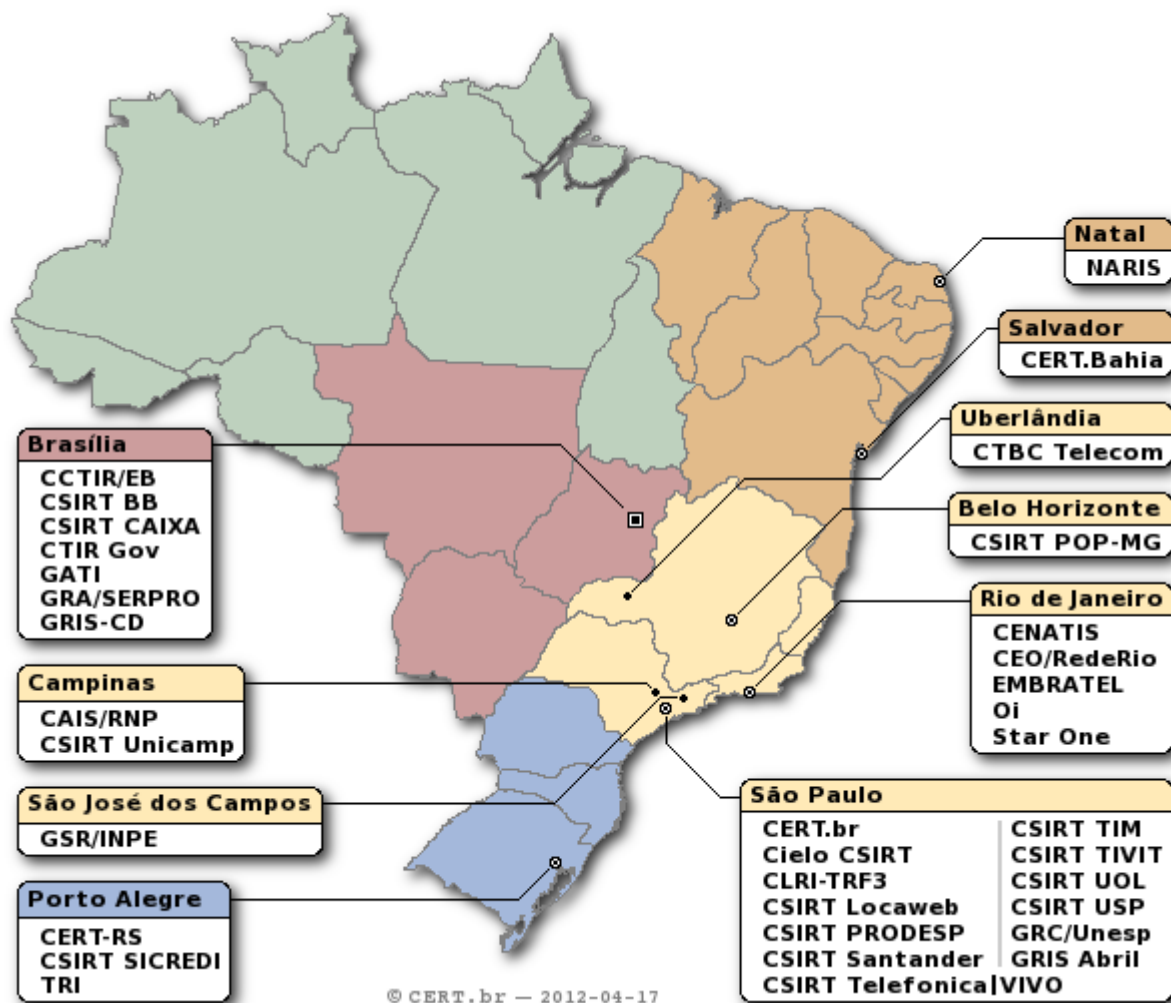
<http://www.enisa.europa.eu/media/press-releases/new-from-enisa-2013-updated-map-inventory-of-europe2019s-201cdigital-fire-brigades201d-with-173-computer-emergency-response-teams-listed/image/image_view_fullscreen>.





6

Poměrně velké množství pracovišť typu CERT/CSIRT se nachází třeba v Brazílii.⁵



Česká republika, země v izolaci?

Česká republika rozhodně nepatří mezi země, které by v rámci Evropy respektive Evropské unie udávaly tón co se týče zřizování pracovišť typu CERT/CSIRT.⁶ To v konečném důsledku nevytváří dobrý obraz o důrazu, kladeném na otázky informační bezpečnosti v České republice.

Je přitom třeba zdůraznit, že konkrétní platforma se CERT/CSIRT pracovištěm stane v okamžiku, kdy jej ostatní již existující CERT/CSIRT pracoviště jako takové akceptují a naváží s ním základní spolupráci.

⁵ Brazilian CSIRTs; in: CERT.br <<http://www.cert.br/csirts/brazil/>>.

⁶ KRULÍK, Oldřich; HNÍK, Václav. Zahraniční inspirace, související s tématem kybernetických hrozeb. Policista. 2007, č. 10, příloha, s. I až XII.

Terena; in: Wikipedia. <<http://en.wikipedia.org/wiki/terena>>.

Cesta k získání statutu CERT/CSIRT pracoviště nemusí být složitá, pokud je na jejím začátku jasným způsobem a pravdivě deklarováno několik klíčových informací:

- **kdo je zřizovatelem a provozovatelem pracoviště;**
- základní kontaktní informace (e-mail pro bezprostřední komunikaci, telefonní číslo, poštovní adresa apod.);
- **pole působnosti (věcný rozsah odpovědnosti) pracoviště;**
- nabízené služby.

Jedním z klíčových předpokladů funkčnosti národního CERT/CSIRT týmu tak je jeho **kvalitní napojení na zahraniční protějšky**, které je zpravidla formalizováno prostřednictvím "**akreditace**" v klíčových nadnárodních strukturách:

- Celosvětově působící asociace FIRST (propojuje více než 200 pracovišť typu CERT/CSIRT).⁷ V lednu 2013 to bylo konkrétně 274 týmů z 59 zemí světa.⁸
- Organizační a certifikační místo pro Evropu TF-CSIRT, spojené s organizací TERENA (v květnu 2009 sdružovalo 144 pracovišť, zatím platný přehled – ze září 2012 – hovoří o 172 akreditovaných subjektech, včetně všech pěti subjektů, uvedených s ohledem na Českou republiku).⁹
- Agentura Evropské unie ENISA¹⁰, která se zaměřuje na informační bezpečnost z hlediska výrobců a provozovatelů.



V průběhu akreditací je ověřována „totožnost, důvěryhodnost a funkčnost“ konkrétního CERT pracoviště. To v praxi znamená, že pracoviště musí dobře zdokumentovat vlastní činnost, musí o sobě zveřejnit základní informace a garantovat obecně akceptovatelné modely chování a odezvy. **Příprava na takový proces zpravidla trvá několik let, proces samotný několik měsíců.** Tento proces je aktuálně třístupňový:

- Rozeznání (akceptace) subjektu (statut „listed“);
- Akreditace;
- Certifikace (podle norem ISO¹¹).

⁷ Forum of Incident Response and Security Teams. <<http://www.first.org/>>.

⁸ Members around the World; in: FIRST <<http://www.first.org/members/map>>.

⁹ Evropská mezinárodní organizace podporující aktivity v oblasti internetu, infrastruktur a služeb v rámci akademické komunity (Trans-European Research and Education Networking Association).

TF-CSIRT Membership; in: Terena, 2012 <<http://www.terena.org/activities/tf-csirt/membership.html>>.

¹⁰ Index Inventory; in: ENISA <http://www.enisa.europa.eu/cert_yinventory/index_inventory.htm>.

¹¹ Například systém řízení kvality (ISO 9001:2008) a informační bezpečnosti (ISO 27001:2005).

Členstvím v těchto organizacích se pak CERT/CSIRT pracovišti otevírá cesta k důležitým a užitečným informacím, které vytvářejí a aktualizují členské týmy, a k užší spolupráci s nimi. Organizace FIRST pořádá jednou ročně pětidenní konferenci, setkání TF-CSIRT se konají třikrát ročně. Setkání vždy hostí jeden z evropských spolupracujících týmů. **V lednu 2008 se toto setkání konalo v České republice**, tuzemskou situaci však příliš neakcelerovalo.¹²

Přitom je třeba zdůraznit, že národní prostředí je v každé zemi natolik specifické, že žádný zahraniční model nelze pro potřeby České republiky plošně a nekriticky přejímat (kopírovat).



Role CERT/CSIRT pracovišť je v mezinárodním kontextu nezastupitelná. **V případě kybernetického útoku, vedeného ze zahraničí, je komunikace po linii CSIRT/CERT pracovišť často rychlejší a efektivnější, než komunikace v rámci policejní spolupráce (a je využitelná i při komunikaci se zeměmi, se kterými žádná policejní spolupráce nefunguje).**

Trnitá cesta ke stanovení vrcholové hierarchie pracovišť typu CERT/CSIRT v České republice

Doba prehistorická

Ačkoli Česká republika je na Internet napojena od roku **1993** respektive **1994**, o komplexní bezpečnostní politice v této oblasti není možné hovořit dodnes. Téma vybudování pracoviště (vrcholové hierarchie pracovišť) typu CERT v České republice přitom patří mezi „chronické“ aspekty úsilí o zvýšení informační bezpečnosti České republiky po déle než 10 let.

Nutnost vybudování vrcholového pracoviště typu CERT/CSIRT v České republice přitom zmiňuje již Harmonogram opatření „Koncepce boje proti trestné činnosti v oblasti informačních technologií“, která byla schválena ministrem vnitra roku **2001**: „*Iniciovat vznik a podporovat činnost skupiny typu CERT jako nevládního sdružení kvalifikovaných odborníků informujících ostatní profesionály o bezpečnostních problémech a reagujících na probíhající útoky.*“ (gesce: Ministerstvo vnitra, ve spolupráci s Úřadem pro veřejné informační systémy, s ministrem vlády a předsedou Rady vlády pro státní informační politiku, Ministerstvem spravedlnosti, Ministerstvem kultury, Ministerstvem školství, mládeže a tělovýchovy a Národním bezpečnostním úřadem; termín: 30. červen **2002**).

Odpovědnost za oblast informační infrastruktury v České republice byla dlouhou dobu předmětem kompetenčních sporů. Mezi lety **2003** až **2007** existovalo Ministerstvo informatiky, které za tuto oblast do značné míry odpovídalo. Po jeho zrušení nebyla agenda v plnosti delimitována a nastalo období sporů, které se vlekly řadu let.

¹² January 2008 FIRST Technical Colloquium <<http://www.first.org/events/colloquia/jan2008>>.

Ministerstvo informatiky ostatně zařadilo do dokumentu „Akční plán plnění opatření Národní strategie informační bezpečnosti České republiky“ (NSIB) obdobné úkoly (původně pro Ministerstvo informatiky, jejichž plnění však ve schválené verzi přešlo na Ministerstvo vnitra): „Realizovat systém včasného varování a reakce. Ustavit národní centrum pro řízení, monitoring a analýzu bezpečnostního prostředí informačních a komunikačních systémů České republiky. Ustanovit pracoviště typu CERT s národní gescí.“ (gesce: Ministerstvo vnitra ve spolupráci s Bezpečnostní informační službou; termín: nejpozději v průběhu roku 2008). „V rámci pracoviště typu CERT zavést monitorování účinnosti navržených protiopatření.“ (gesce: Ministerstvo vnitra; termín: nejpozději v průběhu roku 2008).

Pilotní pracoviště a jeho konkurenti

Od roku **2006**, respektive **2007** se do procesu budování Národního pracoviště typu CSIRT/CERT zapojilo **Konsorcium**, které zvítězilo ve výběrovém řízení na projekt Bezpečnostního výzkumu Ministerstva vnitra pro roky 2007 – 2010 „Problematika kybernetických hrozeb z hlediska bezpečnostních zájmů České republiky“.¹³ Součástí Konsorcia byl i tým CESNET-CERTS, tedy první domácí subjekt typu CSIRT/CERT, disponující příslušnými praktickými zkušenostmi, napojený na relevantní nadnárodní platformy. Proces budování „**koordinačního modelového pracoviště typu CSIRT**“ (CSIRT.CZ) v prostorách CESNET započal v polovině roku **2007**. Dne 3. dubna **2008** byl spuštěn jeho pilotní provoz. Pracoviště průběžně pořádalo metodická zaměstnání (za účasti řady soukromých subjektů, zástupců Bezpečnostní informační služby, Policie České republiky a Národního bezpečnostního úřadu). Tým CSIRT.CZ za dobu své existence získal určité renomé doma (klíčové firmy) i v zahraničí, ale jeho formální mezinárodní akreditaci brání jednak nejistota o jeho budoucnosti po skončení projektu.

Určitou slepou uličkou v této oblasti představovala paralelní aktivita firmy Relsie, která v únoru **2007** uzavřela s Ministerstvem vnitra memorandum o porozumění (v příloze), ve kterém se zavazuje vybudovat střešové pracoviště typu CERT/CSIRT pro Českou republiku (CERT.ORG). V této oblasti přitom firma do té doby v zásadě nepodnikala a pro zahraniční partnery byla de facto neznámým hráčem.¹⁴



Pro zahraničí se tak situace v České republice stala ještě více nečitelnou a dva konkurenční týmy byly pro případné partnery matoucí.

Od září **2008** funguje i bezpečnostní tým sdružení NIC.CZ (**CZ.NIC-CSIRT**). **Efektivita tohoto týmu se zatím jeví být objektivně nejvyšší ze všech týmů tohoto typu v České republice.**

¹³ Konsorcium tvořily tyto subjekty: několik fakult University Karlovy, Českého vysokého učení technického, sdružení CESNET a společnosti NESS Czech. Konsorcium v rámci projektu bezpečnostního výzkumu řeší i další úkoly, které s budováním pracoviště typu CERT/CSIRT nesouvisí.

Problematika kybernetických hrozeb; in: Ministerstvo vnitra <<http://www.mvcr.cz/clanek/vysledky-projektu.aspx>>.

¹⁴ Pilotní kurz CERT – TERENA <<http://www.relsie.cz/rj/pilotni-kurz-cert-terena>>.

Řadu incidentů (například na rozdíl od CSIRT.CZ) pouze „nesleduje“ a „nearchivuje“, ale rázně řeší odpojením sítě, která se učitým způsobem zpronevěřila platným pravidlům.

Navzdory všem dílčím úspěchům se od roku 2007 až do počátku roku 2010 nepodařilo docílit politické shody ohledně praktických kroků při budování národního pracoviště typu CERT/CSIRT. V poslední fázi si odpovědnost (a náklady), které byly s tímto krokem spojeny, navzájem „přehazovaly“ subjekty jako Ministerstvo vnitra, Ministerstvo obrany či Národní bezpečnostní úřad. Není divu, že tyto prodlevy byly s rozpaky komentovány v domácím odborném tisku.¹⁵

Překlenutí kompetenčního vakua

Jasno (alespoň na čas) do celé věci vnesla až „úřednická vláda“, konkrétně usnesení Bezpečnostní rady státu ze dne 5. ledna 2010 č. 4, k Analýze aktuální úrovně zajištění kybernetické bezpečnosti České republiky. To ukládá hlavní gesci za další kroky jednoznačně Ministerstvu vnitra.¹⁶

V přímé návaznosti na výše uvedené usnesení Bezpečnostní rady státu byl počátkem roku 2010 v rámci Ministerstva vnitra ustaven nový odbor nazvaný **odbor kybernetické bezpečnosti**.¹⁷ Jednou z jeho prvních registrovatelných aktivit byla dne 25. března 2010 účast na jednání Pracovní skupiny CSIRT.CZ, jejímiž členy jsou zástupci významných provozovatelů sítí, poskytovatelů obsahu, rizikových služeb, bezpečnostních složek České republiky, Českého telekomunikačního úřadu, sdružení CZ.NIC i NIX.CZ a akademického sektoru.¹⁸

Ze strany státu (resortu vnitra) se ani poté však neudály žádné hmatatelné kroky, proto tedy **iniciativu převzal soukromý sektor, konkrétní regulátor firma CZ.NIC**. Ten na vlastní náklady a odpovědnost vytvořil pracoviště typu CERT/CSIRT, které využívalo zázemí této firmy a sloužilo nejširší veřejnosti ve státě a to až do **16. prosince 2010, kdy bylo podepsáno Memorandum o Computer Security Incident Response Team České republiky**¹⁹ mezi Ministerstvem vnitra a CZ.NIC, podle kterého správce české národní domény (CZ.NIC) přebírá od 1. ledna 2011 agendu národního bezpečnostního týmu CSIRT.CZ.²⁰

¹⁵ DOČEKAL, D., CSIRT.cz přichází. Kyberzločincům navzdory. <<http://www.lupa.cz/clanky/csirt-cz-prichazi-kyberzlocincum-navzdory/>>.

MALÝ, O., Stát chce bojovat s kyberzločinem; in: Lidové noviny.

<http://www.cesnet.cz/sdruzeni/napsali-o-nas/2010/02/20100210_Lidove_noviny.html>.

¹⁶ Záznam ze schůze Bezpečnostní rady státu ze dne 5. ledna 2010.

<<http://www.vlada.cz/cz/ppov/brs/cinnost/zaznamy-z-jednani/zaznam-ze-schuze-brs-konane-dne-5--ledna-2010-66950/>>.

¹⁷ Ministerstvo vnitra: odbor kybernetické bezpečnosti.

<<http://www.mvcr.cz/clanek/odbor-kyberneticke-bezpecnosti.aspx>>.

Pracovní skupina CSIRT.CZ o vládním bezpečnostním pracovišti CSIRT.

<<http://www.cesnet.cz/doc/tisk/2010/tz100330.html>>.

Ministerstvo vnitra představí návrh řešení kybernetické bezpečnosti ČR, Zpravy.rozhlas.cz.

<http://www.rozhlas.cz/zpravy/spolecnost/_zprava/706944>.

¹⁸ SecurityWorld. Ministerstvo vnitra chce zřídit CSIRT, vládní pracoviště pro bezpečnost IT.

<<http://securityworld.cz/aktuality/ministerstvo-vnitra-chce-zridit-csirt-vladni-pracoviste-pro-bezpecnost-it-2498>>.

Pracovní skupina CSIRT.CZ o vládním bezpečnostním pracovišti CSIRT.

<<http://www.cesnet.cz/doc/tisk/2010/tz100330.html>>.

¹⁹ Memorandum o Computer Security Incident Response Team České republiky: Memorandum o CSIRT České republiky.

²⁰ CZ.NIC ohlídá kybernetickou bezpečnost České republiky. <<http://www.nic.cz/page/830/cz.nic-will-watch-over-cybernetic-security-of-the-czech-republic>>.

V Memorandu je vedle toho uvedeno, že Ministerstvo vnitra řeší postavení pracovišť typu CERT/CSIRT v rámci státní správy a snaží se podpořit zařazení CSIRT.CZ do mezinárodních struktur, a to zejména tím, že potvrdilo statut CSIRT.CZ jako národního CSIRT týmu. Dále koordinuje činnost CSIRT.CZ, vyhodnocuje informace, které obdrží od CSIRT.CZ v případě, že CSIRT.CZ má podezření, že řešený incident může mít dopad na systémy státu, respektive státní správy, a má právo požádat o provedení auditu výkonu činnosti CSIRT.CZ (v tomto případě je sdružení CZ.NIC povinné audit provést a o jeho výsledku informovat Ministerstvo vnitra).²¹ Ministerstvo vnitra bude podporovat sdružení CZ.NIC jen v případě, že prostředky na financování CSIRT.CZ získá z fondů Evropské unie či mezinárodních organizací.²²

„CSIRT.CZ byl výzkumný úkol provozovaný jako součást projektu kybernetické hrozby sdružením CESNET. Tento projekt končí k 31. prosinci 2010. Od 1. ledna 2011 na základě dohody odboru kybernetických hrozeb Ministerstva vnitra, sdružení CESNET a CZ.NIC přebírá projekt správce národní domény. To, že se podařilo zachovat kontinuitu provozu pracoviště CSIRT.CZ i do dalšího období, je dobrá zpráva nejen pro českou internetovou komunitu.“²³

CSIRT.CZ, který byl mezinárodní infrastrukturou vnímán již od svého vzniku jako tzv. „v podstatě národní CSIRT tým“ (de facto national), se stal za Českou republiku už v roce 2010 spolupracovníkem unijní agentury ENISA²⁴.



Ilustrace: Jedním z hnacích motorů celého úsilí není nikdo menší než Andrea Kropáčová, růže mezi trním domácí kyberkomunity.

V souvislosti s výše uvedenými skutečnostmi Bezpečnostní rada státu projednala 28. února **2011** materiál o aktuálním stavu řešení problematiky kybernetické bezpečnosti České republiky. Vzhledem k důležitosti kybernetické bezpečnosti je připravována Strategie pro oblast kybernetické bezpečnosti, která by měla být předložena ministrem vnitra na schůzi

²¹ Memorandum o Computer Security Incident Response Team České republiky. <http://www.nic.cz/files/nic/doc/Memorandum_CSIRT.CZ.pdf>.

²² Memorandum o Computer Security Incident Response Team České republiky. <http://www.nic.cz/files/nic/doc/Memorandum_CSIRT.CZ.pdf>.

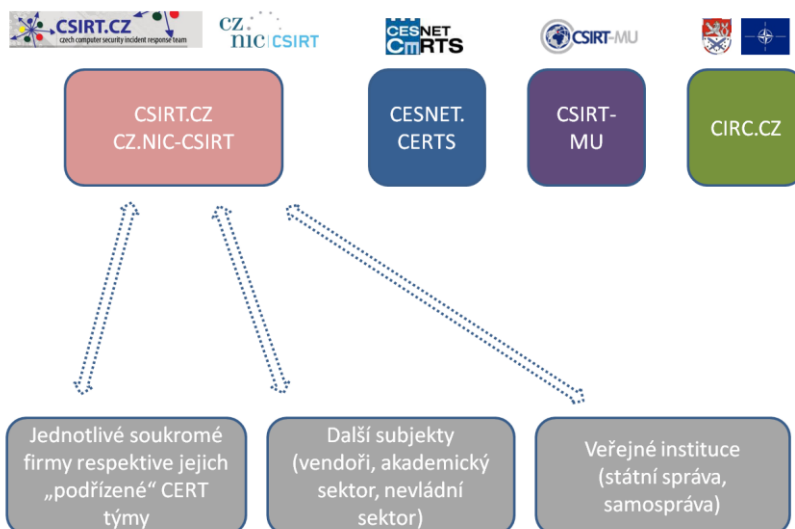
²³ MACÍCH, J., CZ.NIC od ledna přebírá agendu CSIRT.CZ; in: Lupa, 17. XII. 2010 <<http://www.lupa.cz/zpravicky/cz-nic-od-ledna-prebira-agendu-csirt-cz/>>.

²⁴ The Czech Republic; in: ENISA <<http://www.enisa.europa.eu/activities/cert/security-month/pilots/czech-republic>>.

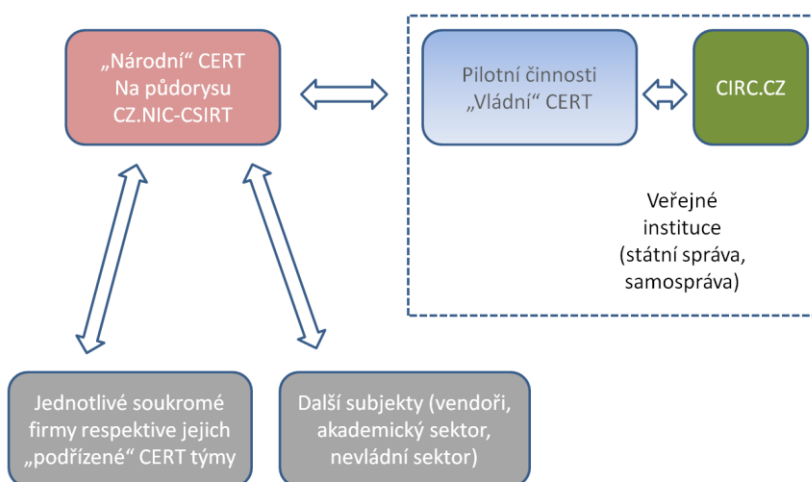
vlády do 30. června 2011, ještě před předložením na schůzi vlády by měla být projednána schůzi Bezpečnostní rady státu.

Perspektivu jednotlivých etap možného vývoje, tak jak se jevíly na počátku roku 2011, zachycují následující vizualizace:²⁵

I. fáze (konce roku 2010), existence několika pracovišť typu CERT/CSIRT, kdy na dvě z nich se může širší veřejnost obracet se svými podněty a problémy.

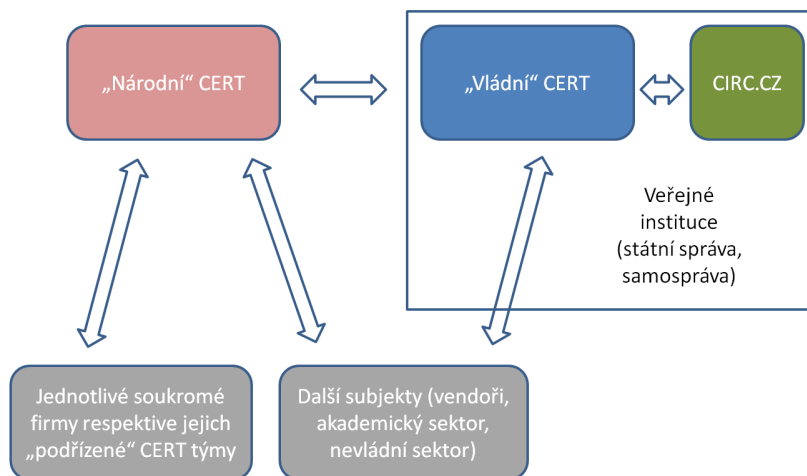


II. fáze: budování „Národního“ pracoviště typu CERT na půdorysu CZ.NIC-CSIRT, postupné vytváření „Vládního“ pracoviště typu CERT.

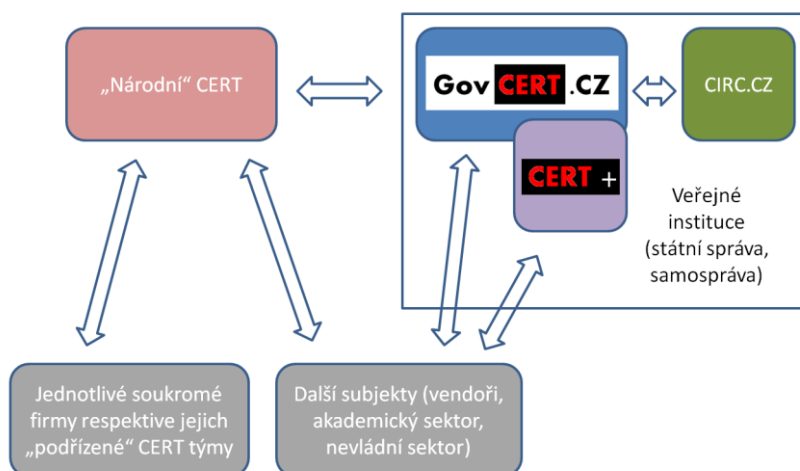


²⁵ Hník, V.; Krulík, O., Okolnosti, související s budováním pracovišť typu CERT v České republice, podklad pro potřeby Ministerstva vnitra, 2010 (včetně autorství „pracovní verze“ loga GovCERT.cz a CERT+..

III. fáze: Jasnější dělba práce mezi oběma vrcholovými pracovišti typu CERT.



IV. fáze: Výsledný stav, plná funkčnost „Vládního“ pracoviště typu CERT (GovCERT.cz) a „Certifikační autority“ (CERT+).



Přesun agendy na Národní bezpečnostní úřad

„Vyjasněná“ gesce Ministerstva vnitra však netrvala dlouho. Na základě **usnesení Vlády České republiky č. 781 ze dne 19. října 2011** došlo ke změně subjektu (střechového gestora a tzv. „národní autority“) odpovědného v rámci veřejného sektoru České republiky za oblast informační („kybernetické“) bezpečnosti. Z Ministerstva vnitra České republiky tento úkol přešel na Národní bezpečnostní úřad. Nový gestor ve sledované oblasti, ať již sám, nebo v součinnosti s dalšími subjekty, vyvíjí činnost v mnoha oblastech.²⁶

²⁶ Informace k usnesení vlády České republiky č. 781 ze dne 19. října 2011; in: Národní bezpečnostní úřad <<http://www.nbu.cz/cs/aktuality/994-informace-k-usneseni-vlady-ceske-republiky-ze-dne-19-rijna-2011-c-781/>>.



Současně vláda zřídila **Radu pro kybernetickou bezpečnost**²⁷ a **Národního centrum kybernetické bezpečnosti**²⁸ jako součásti Národního bezpečnostního úřadu²⁹. Národnímu bezpečnostnímu úřadu zároveň vláda uložila řadu konkrétních úkolů. Za koordinace Národního bezpečnostního úřadu sice vznikl strategický dokument pro roky 2012 až 2015.³⁰

V lednu **2012** CSIRT.CZ zhodnotil rok svého dosavadního fungování po uzavření prvního Memoranda – mimo jiné – následovně:³¹

„Tým CSIRT.CZ má v současné době oficiálně čtyři členy, kteří zajišťují provoz týmu a reprezentaci týmu ve světě ... Osvětová činnost, národní a mezinárodní spolupráce jsou nedílnou součástí činnosti každého pracoviště typu CERTS/CSIRT, obzvláště těch s národním nebo vládním mandátem, které hovoří za danou zemi na příslušných mezinárodních fórech a jsou také prvním logickým kontaktním místem pro získání informací o stavu bezpečnosti ICT dané země ... V červenci 2011 jsme uspořádali pilotní školení „Světlem Internetu a domén“. Školení je určené zaměstnancům státní správy a členům bezpečnostních složek, zejména složkám Policie ČR. Plníme tím závazek vzdělávat a spolupracovat s bezpečnostními složkami ČR a státní správou na poli zlepšování bezpečnostní situace v sítích provozovaných v ČR. Speciální pozornost je v kurzu věnována praktickým záležitostem, které by měly pomoci (zejména) vyšetřovatelům Policie ČR orientovat se v problematice základních typů počítačové kriminality a naučit je obracet se přímo na konkrétní subjekty, které mohou pomoci při jejich práci. Účastníky pilotního kurzu byli členové BIS (Bezpečnostní informační služba) a sloužil především k získání zpětné vazby od účastníků, kteří nám v závěrečné diskusi poskytli celou řadu cenných námětů pro zlepšení obsahu jednotlivých přednášek z oblasti organizace Internetu, provozu sítí a služeb, práva apod. ... V roce 2011 jsme byli vyzváni k účasti v expertní pracovní skupině ENISA zabývající se spoluprací mezi světem orgánů činných v trestním řízení (LEA, Law Enforcement Authorities) a světem CERT/CSIRT týmů v oblasti boje proti kyberkriminalitě. Výsledkem práce této expertní skupiny bude dokument mapující

²⁷ Rada na svém zasedání dne 23. XI. 2011 mimo jiné přijala usnesení o harmonogramu budování Národního centra kybernetické bezpečnosti.

Rada pro kybernetickou bezpečnost; in: Národní centrum kybernetické bezpečnosti
<<http://www.govcert.cz/cs/rkb/rada-pro-kybernetickou-bezpecnost/>>.

Národní centrum kybernetické bezpečnosti se představuje a nabízí zajímavé pracovní příležitosti; in: České vysoké učení technické <<http://oi.fel.cvut.cz/en/node/621>>.

²⁸ Národní centrum kybernetické bezpečnosti <<http://www.govcert.cz/cs/>>.

²⁹ Národní bezpečnostní úřad <<http://www.nbu.cz/cs/>>.

³⁰ Zprávy Ministerstva vnitra o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky.

Ministerstvo vnitra: Statistiky kriminality – dokumenty

<<http://www.mvcr.cz/clanek/statistiky-kriminality-dokumenty.aspx>>.

³¹ . CSIRT.CZ a jeho první rok fungování v roli Národního CSIRT České republiky; in: CSIRT.cz, 12. I. 2012
<<http://csirt.cz/page/992/csirt.cz--a-jeho-prvni-rok-fungovani-v-rol-narodniho-csirt-ceske-republiky/>>.

zkušenosti získané od existujících týmů na obou stranách (LEA a CERT/CSIRT), sada doporučení a především podklad pro další práci.“³²

Perspektiva ukončení výše uvedeného stavu v průběhu roku 2012 se nenaplnila. Národní bezpečnostní úřad zatím nespustil svůj GovCERT, budovaný v někdejších prostorách Ministerstva obrany v Brně.³³ Výsledkem situace bylo další Memorandum, které tento zlomový okamžik přesouvá do roku 2015. Do té doby bude bezpečnost kyberprostoru státu dominantně záviset na firmě NIC.CZ.³⁴

„Současné řešení ochrany kyberprostoru je nevyhovující. CSIRT.CZ sdružení CZ.NIC je kvalitní a profesionální, ani tato skutečnost ovšem nemůže suplovat absenci vládního týmu CERT, který musí být součástí bezpečnostního systému a ochrany kyberprostoru ... Podobně situaci vidí členové národního CSIRTu sdružení CZ.NIC, který je sice tvořen špičkovými odborníky, ale nemá žádné pravomoci ani odpovědnost, které jsou v případě ohrožení bezpečnosti klíčové. CSIRT má, jako jediná instituce, která se bezpečností českého kyberprostoru zabývá, pouze poradní roli ... Do té doby se budou o bezpečnost českého kyberprostoru starat čtyři odborníci CZ.NIC s polovičním úvazkem, kteří nemají oprávnění pracovat s utajovanými informacemi a ze zákona žádné pravomoci ... Postupem času jim budou schopni pomoci nebo je nahradit zaměstnanci brněnského vládního Centra, bez opory v legislativě to však stále bude jen skupina odborníků, se kterými se nikdo nemusí bavit.“

Jak bude vypadat výsledný stav?

Současný návrh zákona o kybernetické bezpečnosti obsahuje návrh rámce zajišťování střežových funkcí v oblasti informační bezpečnosti v České republice. Odbornou veřejností je tento návrh chápán jako posun pozitivním směrem (ve srovnání s mnohaletou nečinností Ministerstva vnitra).³⁵ Předpokládáno je **vytvoření dvou vrcholových CERT týmů v České republice.**

³² CSIRT.CZ a jeho první rok fungování v roli Národního CSIRT České republiky; in: CSIRT.cz, 12. I. 2012 <<http://csirt.cz/page/992/csirt.cz--a-jeho-prvni-rok-fungovani-v-rol-i-narodniho-csirt-ceske-republiky/>>.

Další hodnocení situace viz:

HOŠT, O., Trendy v bezpečnosti 2012: soukromí, Facebook, mobilní platby a stará dobrá havěť; in: Lupa.cz, 2. III. 2012 <<http://www.lupa.cz/clanky/trendy-v-bezpecnosti-2012-soukromi-facebook-mobilni-platby-a-stara-dobra-havet/>>.

Česká kybernetická jednotka CSIRT bojuje proti Anonymous; in: Zive.cz, 2. II. 2012 <<http://www.monitoruji.cz/it-pocitace/565556/ceska-kyberneticka-jednotka-csirt-bojuje-proti-anonymous>>.

Jak CSIRT.CZ došel k akreditaci; in: Lupa.cz, 1. XI. 2011 <<http://www.monitoruji.cz/it-pocitace/510651/jak-csirt-cz-dosel-k-akreditaci>>.

Českou republiku; in: Aktualne.cz, 21. XI. 2011 střeží před kyberútokem čtyři lidé na půl úvazku <<http://www.monitoruji.cz/it-pocitace/523094/cr-strezi-pred-kyberutokem-ctyri-lide-na-pul-uvazku>>.

CZ.NIC převezme systém řešení bezpečnostních incidentů CSIRT; in: CeskeNoviny.cz, 16. XII. 2010 <<http://www.monitoruji.cz/it-pocitace/349997/cz-nic-prevezme-system-reseni-bezpecnostnich-incidentu-csirt>>.

³³ Vládní CERT (Computer Emergency Response Team); in: Národní bezpečnostní úřad <<http://www.govcert.cz/cs/govcert/>>.

³⁴ KOVALÍK, J., Česko se začne před kyberútoky bránit až v roce 2015; in: DataRama, 6. XII. 2011 <<http://datarama.aktualne.centrum.cz/clanek.phtml?id=723306>>.

³⁵ Zároveň je však uváděno, že tento koncept by mohl být v určitých ohledech vylepšen a připodobněn stavu v zemích, které jsou v oblasti informační bezpečnosti mnohem dál (například Německo a Bundesamt für Sicherheit in der Informationstechnik (BSI), <http://www.bsi.bund.de>).

Bürger-CERT; in: Bundesamt für Sicherheit in der Informationstechnik <<https://www.buerger-cert.de/>>.

„**Národní**“ **CERT** bude vybudován na půdorysu (základě) pracoviště soukromé firmy, regulátora odpovědného za doménu .cz, firmy CZ.NIC, nazvaného CZ.NIC-CSIRT. Stane se tak za využití zkušeností modelového pracoviště, provozovaného v rámci výzkumného projektu Ministerstva vnitra firmou CESNET (CSIRT.CZ). „Národní“ CERT naváže nebo prohloubí existující vazby s obdobnými týmy v rámci soukromého (Network Monitoring Cluster) a v první fázi zřejmě i veřejného sektoru. CSIRT.CZ se bude jako národní tým podílet na řešení incidentů týkajících se kybernetické bezpečnosti v sítích provozovaných v České republice. CSIRT.CZ bude poskytovat při řešení incidentů koordinační pomoc, nikoliv fyzickou podporu, tato pomoc přitom nebude poskytována přímo koncovým uživatelům. CSIRT.CZ bude shromažďovat a vyhodnocovat data o oznámených incidentech a předávat hlášené incidenty osobám zodpovědným za chod sítě (služby), která je zdrojem daného incidentu a to v souladu se závažností incidentu.³⁶ CSIRT.CZ bude plnit roli tzv. národního PoC (Point of Contact) pro oblast informačních technologií, bude centrem vzdělávání a šíření osvěty v oblasti kybernetické bezpečnosti bude umožňovat spolupráci na národní i mezinárodní úrovni, výměnu zkušeností a informací a pomáhat se zřizováním CERT/CSIRT týmů v sítích provozovaných v České republice a pomáhat jim s navázáním spolupráce se světovými bezpečnostními platformami.³⁷

Zároveň (nebo později) by bylo zahájeno **budování „vládního“ CERT týmu (GovCERT.CZ³⁸)**, za přímého využití kapacit Ministerstva vnitra. Toto pracoviště bude primárně určeno k monitoringu vládních sítí a (veřejné) kritické informační infrastruktury, respektive ke koordinaci a metodickému vedení dalších dílčích center tohoto typu, které fungují či budou fungovat v rámci konkrétních veřejných institucí. V souvislosti s budováním tohoto pracoviště bude zejména potřeba:

Vazby obou subjektů (zejména „vládního“ pracoviště) na „armádní“ pracoviště obdobného typu (CIRC.CZ) budou předmětem dalších jednání v rámci relevantních pracovních skupin.

Pro aktuálně navrhovaný model je typická dělba práce mezi:

- veřejným sektorem (Národní centrum kybernetické bezpečnosti – NCKB – jako integrální součást Národního bezpečnostního úřadu,³⁹ národní dohledové centrum pro boj s kybernetickými hrozbami,⁴⁰ v zahraničí obvykle označované za vládní, GovCERT);
- soukromým sektorem (ústřední dohledové centrum pro boj s kybernetickými

³⁶ Memorandum o Computer Security Incident Response Team České republiky. <http://www.nic.cz/files/nic/doc/Memorandum_CSIRT.CZ.pdf>.

³⁷ Memorandum o Computer Security Incident Response Team České republiky. <http://www.nic.cz/files/nic/doc/Memorandum_CSIRT.CZ.pdf>.

³⁸ Vzhledem ke skutečnosti, že v České republice již existuje několik platform, nesoucích v názvu zkratku CERT respektive CSIRT, došlo k rozhodnutí tento „vládní“ koncept odlišit (podobně jako v jiných zemích světa) předponou „Gov“ (ze slova „government“ tedy „vládní“). Tento výraz navíc naznačuje „nadřazenost“ takové platformy nad ostatními CERT-y (CSIRT-y), existujícími v rámci státu.

³⁹ Národní centrum kybernetické bezpečnosti se bude údajně snažit ochránit především sítě v rámci veřejných institucí, například ministerstev, energetických podniků, nemocnic nebo České národní banky. Národní centrum kybernetické bezpečnosti (je ve svém zárodečném stavu podřízeno přímo řediteli Úřadu.

⁴⁰ CERT (Cybernetic Emergency Response Team, „Hlásné středisko při kybernetických ohroženích“) je subjekt, odpovědný za příjem, posouzení a řešení hlášení o bezpečnostních incidentech v konkrétní počítačové síti.

hrozbami, „Network Monitoring Center“, sloužící převážně soukromým firmám jako jsou banky a podobně, v zahraničí obvykle označované za Národní CERT).

Oba vrcholové týmy je třeba chápat v první řadě jako partnery, kteří si navzájem „odlehčují“ agendu. GovCERT by nicméně disponoval právem veta v řadě ohledů, ale zároveň nedisponuje (a je otázka, zda do roku 2015, kdy se předpokládá jeho plná funkcionality, bude disponovat) zdaleka takovými technickými a lidskými kapacitami (je údajně problém naplnit příslušná tabulková místa) a mezinárodními kontakty, jako Národní CERT, budovaný převážně po linii firmy CZ.NIC. Celý proces budování této platformy bude zřejmě postupovat od „omezenějších“ k „ambicióznějším“ cílům.

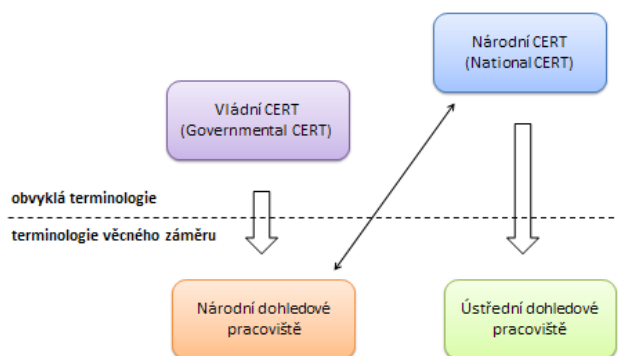
Věcný záměr zákona o kybernetické bezpečnosti je zatím jen jakýmsi náčrtem požadovaného „toku“ údajů a hlášení v jednom směru, a opatření a protipopatření ve druhém směru. Nejsou zcela jasné hranice toho, koho se vše týká (významné a nevýznamné informační systémy veřejné správy, a „vybrané“ poskytovatele služeb a provozovatele sítí). To vše bez přesnějšího definování toho, co bude po příslušných subjektech požadováno, v rámci určitých bezpečnostních opatření a protipopatření.

Celá tato vize byla obšírně komentována domácí expertní komunitou jako poněkud nestandardní:⁴¹

„Ve světě informační bezpečnosti existují určité zaběhnuté termíny (viz třeba výstupy ENISA) ... „podle kterých se přívlastkem „národní“ označuje ten CERT či CSIRT, který stojí v celé hierarchii CERTů a CSIRTů v konkrétní zemi nejvýše a stará se obecně o všechny zdejší systémy. Stejně tak je hlavním kontaktním místem pro komunikaci se zahraničím, s CERTy a CSIRTy v jiných zemích, a je také hlavním zástupcem své země v mezinárodních organizacích, které se zabývají kybernetickou bezpečností. Vedle „národního“ CERTu či CSIRTu mnohde existují ještě „vládní“ (governmental) CERTy/CSIRTy, které se starají o ty systémy, které spadají do oblasti veřejné správy (státní správy i samosprávy). Typicky přitom mají poněkud odlišné pravomoci a způsob fungování než národní CERT/CSIRT, protože stát si vůči „svým“ systémům obvykle může (a chce) dovolit jiný režim dohledu. V praxi přitom nemusí být „národní“ a „vládní“ CERT/CSIRT různé subjekty. Jejich role může být kombinována v rámci jednoho subjektu. Nicméně zde popisovaný návrh věcného záměru jakoby obrací logiku obou přívlastků – když to, co je obvykle „vládní“, označuje naopak jako „národní“ (a to, co je obvykle „národní“, označuje jako „ústřední“) ... Není to přitom tak, že by autoři návrhu neznali obvyklou terminologii. Právě naopak, když své názvy definují, sami upozorňují na to, že se liší od obvyklé terminologie ... Povšimněme si ještě jedné věci: že ono „národní“ dohledové pracoviště (správně „vládní“ CERT) bude vlastně „vnořeno“ do jiného pracoviště, konkrétně do Národního centra kybernetické bezpečnosti. A teprve to bude navázáno na zahraničí, se kterým má zajišťovat onu mezinárodní spolupráci. Navíc i toto Národní centrum bude samo „vnořeno“ do NBÚ, jako jeho organizační součást, a řada „vnitrostátních“ aktivit a vazeb v oblasti kybernetické bezpečnosti bude vycházet či směřovat nikoli k „národnímu“ dohledovému pracovišti (správně „vládnímu“ CERTu), ale přímo k NBÚ

⁴¹ PETERKA, J., Jaký bude zákon o kybernetické bezpečnosti; in: Lupa.cz, 22. II. 2012
<<http://www.lupa.cz/clanky/jaky-bude-zakon-o-kyberneticke-bezpecnosti/>>.

jako takovému ... Bude ale zahraničí rozumět takovéto netradiční struktuře, až o něco doopravdy půjde?“



Vedení CSIRT.CZ respektive NIC.CZ si je takové situace vědomo a snažilo se výše uvedené komentáře „uklidnit“: „**Týmy označované jako vládní a národní** mají v bezpečnostní infrastruktuře CERT/CSIRT týmů zcela specifickou roli. **Týmy označované jako vládní** jsou obvykle určené pro dohled nad sítěmi státní správy, samosprávy a tzv. kritické infrastruktury¹ země. Ve svém poli působnosti jsou chápány jako týmy interního typu – s možností a povinností v případě problému zasáhnout ... **Národní týmy** v prostředí svých zemí obvykle plní především roli národního PoC (Point of Contact), místa pro sdílení informací s ostatními světovými týmy a se subjekty a organizacemi země své působnosti. Na základě znalostí světové infrastruktury a vazeb udržovaných v domácím prostředí je primární rolí týmu efektivně nastavit a zprostředkovat komunikační kanály mezi zainteresovanými subjekty, například v okamžiku řešení vážného, často plošného, bezpečnostního incidentu, který ohrožuje počítačovou infrastrukturu země. Je nutné zdůraznit, že národní CERT/CSIRT není primárně určen k fyzickému řešení konkrétních zaznamenaných problémů (incidentů) ... **Ve světě je provozováno několik týmů, které jsou označené jako vládní nebo národní a vykonávají i roli toho druhého. Obdobný model je v současné době použit v České republice – tým CSIRT coby Národní CSIRT České republiky plní, dočasně dle Memoranda do poloviny roku 2012, také roli vládního týmu.**“⁴²

⁴² CSIRT.CZ a jeho první rok fungování v roli Národního CSIRT České republiky; in: CSIRT.cz, 12. I. 2012 <<http://csirt.cz/page/992/csirt.cz--a-jeho-prvni-rok-fungovani-v-rol-narodniho-csirt-ceske-republiky/>>.

Rámeček: Kontaktní údaje pracovišť typu CERT/CSIRT v České republice

CESNET-CERTS

CESNET, z. s. p. o., Žitná 4, 160 00 Praha 6
telefon: 00 420 224 352 994
e-mail: certs@cesnet.cz
<http://www.csirt.cesnet.cz>
<https://www.trusted-introducer.org/teams/cesnet-certs.html>
ustaven v lednu 2004; akreditován 27. I. 2008
provozován sdružením CESNET a jeho hlavním úkolem je řešení a koordinace řešení bezpečnostních incidentů v síti národního výzkumu CESNET2



CZ.NIC-CSIRT

CZ.NIC, z. s. p. o., CSIRT Team, Americká 23, 120 00 Praha 2
telefon: 00 420 222 745 111
fax: 00 420 222 745 112
e-mail: csirt@nic.cz
<http://www.nic.cz/csirt/>
<https://www.trusted-introducer.org/teams/cznic-csirt.html>
ustaven v červnu 2008, akreditován 26. VIII. 2010
bezpečnostní tým regulátora odpovědného za doménu .cz, sdružení NIC.CZ



CSIRT-MU

CSIRT-MU, Botanická 554/68a, 602 00 Brno
telefon: 00 420 549 494 242
e-mail: csirt@muni.cz
<http://www.muni.cz/ics/services/csirt?lang=cs>
<https://www.trusted-introducer.org/teams/csirt-mu.html>
ustaven v červnu 2009; akreditován jako kandidát 4. XI. 2010, plně akreditován v únoru 2011
pokrývá Masarykovu universitu v Brně



CSIRT.CZ

CSIRT.CZ, CZ.NIC, z. s. p. o., Americká 23, 120 00 Praha 2
telefon: 00 420 222 745 111; 00 420 222 745 111
e-mail: abuse@csirt.cz (v souvislosti s incidenty)
e-mail: info@csirt.cz (jakákoli další komunikace).
<https://www.csirt.cz/>
ustaven v dubnu 2008 jako koordinační modelové pracoviště CSIRT.CZ v rámci CESNET, později řenesen do prostředí CZ.NIC, akreditován v říjnu 2011; na základě Memoranda uzavřeného mezi CZ.NIC a Národním bezpečnostním úřadem vykonává tento subjekt dočasně roli „vládního CSIRT-týmu“



ACTIVE24-CSIRT

ACTIVE 24, s. r. o., Sokolovská 394/17, 186 00 Praha 8
csirt@active24.cz
telefon: 00 420 234 262 077; 00 420 605 204 530
<http://www.active24.cz/csirt>
<https://www.trusted-introducer.org/teams/teams-a.html#active24-csirt>
ustaven v únoru 2012 jako „první CSIRT v rámci komerční firmy v České republice“⁴³



⁴³ Active 24 startuje svůj oficiální bezpečnostní tým; in: Active 24, 13. II. 2012

<<http://www.active24.cz/o-spolecnosti/media/tiskove-zpravy-2012/active-24-startuje-svuj-oficialni-bezpecnostni-tym/>>.

Rámeček: Další významní aktéři: platformy CZ.NIC a NIX.CZ



CZ.NIC

CZ.NIC je zájmové sdružení právnických osob založené roku 1998 předními poskytovateli internetových služeb (dnes se jedná o cca. 80 členů). Hlavní činností sdružení je provozování registru doménových jmen .CZ a 0.2.4.e164.arpa (ENUM⁴⁴), zabezpečení provozu domény nejvyšší úrovně CZ a osvěta v oblasti doménových jmen.⁴⁵

V současné době se sdružení věnuje rozšiřování systému ENUM, rozšiřování a vylepšování systému správy domén, zavádění DNSSEC⁴⁶ a podpoře nových technologií a podpoře projektů prospěšných pro internetovou infrastrukturu v České republice. CZ.NIC je členem mezinárodních organizací, které sdružují obdobné organizace ve světě (CENTR, ccNSO a dalších), a také členem sdružení EURid, spravujícího evropskou doménu .eu.⁴⁷



NIX.CZ

Zájmové sdružení právnických osob NIX.CZ (Neutral Internet Exchange), sdružuje poskytovatele Internetových služeb v České republice s cílem propojení jejich internetových sítí. Sdružení vybudovalo neutrální výměnný uzel Internetu NIX.CZ (Neutral Internet eXchange) v České republice, prostřednictvím kterého mohou být vzájemně propojeny internetové sítě jednotlivých poskytovatelů v České republice.

Telekomunikační společnosti působící v České republice tvoří toto sdružení, protože mají společný zájem na tom, aby byly jejich počítačové sítě vzájemně kvalitně propojeny a jejich zákazníci mohli rychle komunikovat v Internetu v rámci České republiky. Členové společně přispívají na technologie, které tvoří neutrální výměnný uzel a na jeho provoz.

⁴⁴ ENUM Telephone Number Mapping: mapování telefonních čísel.

⁴⁵ O sdružení. <<http://www.nic.cz/page/351/>>.

⁴⁶ DNSSEC (Domain Name System Security Extensions): rozšíření systému doménových jmen (DNS), které zvyšuje jeho bezpečnost. DNSSEC poskytuje uživatelům jistotu, že informace, které z DNS získal, byly poskytnuty správným zdrojem, jsou úplné a jejich integrita nebyla při přenosu narušena.

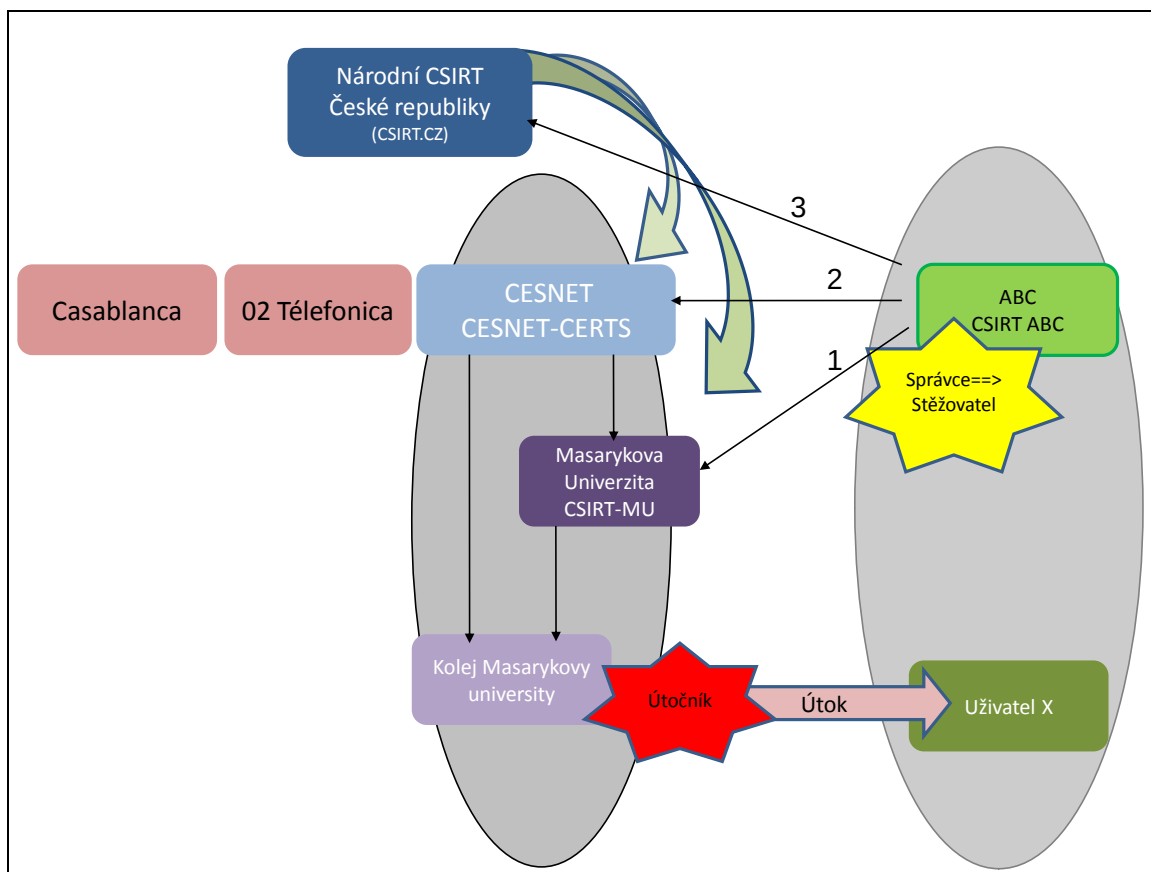
⁴⁷ O sdružení. <<http://www.nic.cz/page/351/>>.

Model možných postupů při hlášení bezpečnostního incidentu

V této části padne zmínka o tom, jak se postupuje a jaké jsou možnosti při hlášení bezpečnostního incidentu a jakou roli v tomto procesu hrají pracoviště typu CERT/CSIRT. Modelový příklad je zasazen do prostředí sítě CESNET2 (kde se nachází útočník) a jednoho fiktivního komerčního operátora – ABC, kde se nachází cíl útoku – uživatel X.

Řekněme, že síť koleje Masarykovy university je veden útok na uživatele X, který se nachází v síti operátora ABC. Uživatel X útok zaregistruje a oznámí ho svému správci – správci sítě, ve které se uživatel X nachází. Správce, kromě základních kroků nápravy, podle zanechaných stop zjistí, že útok je veden z koleje Masarykovy university. Dále zjišťuje, kdo je za provoz kolejní sítě na Masarykově universitě zodpovědný – ideálně jestli existuje CERT/CSIRT tým, který by tuto kolej měl ve sféře svého vlivu. Zjistí, že síť na koleji Masarykovy university je ve sféře vlivu CERT/CSIRT týmu Masarykovy university, který se jmenuje CSIRT-MU

V tento okamžik se ze správce stává tzv. stěžovatel. Obrátí se tedy se stížností na situaci a žádostí o zjednání nápravy na CSIRT-MU. V ideálním případě CSIRT-MU problém vyřeší, tedy nalezne (identifikuje) zdroj útoku, odpojí jej od sítě a zjedná nápravu.



Pozn. Casablanka nevytvořila oficiálně konstituovaný CERT/CSIRT tým, ale provozuje tzv. Bezpečnostní oddělení, nebo tým lidí, kteří se zabývají bezpečnostními otázkami sítě

Casablanky. Takové oddělení nebo tým je de facto CERT/CSIRT týmem, ale nekonstituoval se v rámci organizace FIRST⁴⁸ nebo TERENA⁴⁹.

Nastane-li stav, kdy CSIRT-MU vzniklou situaci neřeší, na stížnost nereaguje nebo problém řešit odmítá, může se stěžovatel obrátit na CERT/CSIRT tým CESNETu (CESNET-CERTS). Jelikož CSIRT-MU je ve sféře vlivu CESNET-CERTS, měl by tým CESNET-CERTS mít k dispozici mechanismy, jak CSIRT-MU k akci přimět, nebo jak problém eliminovat (např. odpojením části problematické sítě).

Ovšem může nastat i třetí případ, kdy problém neřeší ani CERT/CSIRT tým CESNETu. Pak správci uživatele X nezbyvá nic jiného, než se obrátit na Národní CERT/CSIRT České republiky (tým CSIRT.CZ), aby se pokusil zasáhnout on. CSIRT.CZ má však pouze koordinační roli. Může tedy pouze tlačít na CSIRT CESNET nebo CSIRT-MU, aby tento problém vyřešily. V žádném případě však nemá pravomoc síť, ve které se útočník nachází (v tomto případě CESNET2), odpojit.

V případě, že by ani Národní CERT/CSIRT České republiky na podnět správce uživatele X nereagoval, zbývá poslední řešení. Správce uživatele X se musí obrátit na Policii České republiky a podat trestní oznámení. Stávající proces oznamování podezření ze spáchání trestného činu je přitom pro veřejnost těžkopádný a zdlouhavý. (Je nutná návštěva na místně příslušné služebně, problémem je také komunikace s policisty, kteří nejsou odborníky na oblast informační kriminality. Řadový policista často ani nerozumí, v čem tkví podstata oznámeného protiprávního jednání v kyberprostoru a tím pádem trestní oznámení zahájí nenáležitým způsobem, který nakonec vede k založení spisu ad acta).

Závěr

V České republice – tedy zemi, která je relativně vysoce „internetizována“, a kde jsou výrazně propagovány projekty jako Datové schránky a CzechPoint – zůstává bezpečnostní aspekt celé problematiky spíše na okraji zájmu a celá země je tak pro své zahraniční protějšky do značné míry nedůvěryhodným partnerem. Přitom v řadě jiných zemí je situace zásadním způsobem odlišná. Například v Nizozemsku je tato oblast ošetřena jak legislativně, tak prostřednictvím praktických kroků. Země investuje nemalé prostředky do ochrany informační infrastruktury.

Instituce veřejného sektoru v rámci České republiky se naopak ve větší míře starají pouze o své vlastní „výseče“ kyberprostoru a celostátní nadstavba zůstává spíše v rukou aktivnějších hráčů ze soukromého sektoru.

Na eventualitu závažnějšího kyberincidentu v České republice nepomýšlejí ani krizové či havarijní plány. V tom je třeba spatřovat zásadní nedostatek zdejšího systému. Lze totiž konstatovat, že v tuto chvíli není ani tolik podstatné, že Česká republika postrádá příslušnou legislativu, ale mnohem závažnější je ta skutečnost, že zatím nebyly vypracovány postupy, jak v konkrétních situacích (scénářích ohrožení informační infrastruktury) postupovat.

⁴⁸ FIRST - Forum for Incident Response and Security Teams: <<http://www.first.org/>>.

⁴⁹ TERENA – Trans-European Research and Education Networking Association: <<http://www.terena.org/>>.

Namísto závěru: Doporučení, související se sledovanou problematikou⁵⁰

- V rámci střežových institucí budovaných v rámci České republiky je třeba řešit konkrétní aspekty agendy, jako řešení, sběr a distribuce informací o hrozbách z/do participujících center; vytvoření registru incidentů, hrozeb a zranitelností, přístupného odpovídajícím subjektům a vybudování pracoviště pro aktivní ochranu kyberprostoru České republiky.
- Je třeba **vyjasnit, jak budou nastavené příslušné komunikační a kompetenční toky uvnitř České republiky i ve vztahu do zahraničí**. Které z pracovišť bude tím, které bude jednotným kontaktním místem pro celou Českou republiku, na které se bude zahraničí obracet? Jak bude probíhat akreditování pracovišť u evropské platformy TERENA?⁵¹
- Vedle budování hierarchie na celostátní úrovni je třeba **budovat jasnou hierarchii odpovědnosti za téma informační bezpečnosti a kriminality v rámci Policie České republiky**. Kvalifikované provázání a zastřešení odborně a kapacitně silného centrálního pracoviště nelze vnímat jen z pohledu struktury Policie České republiky, ale je třeba poukázat na stávající potřebu řešení součinnosti s ostatními subjekty státní správy a komerční sféry.
- Mimo Policii České republiky je pak na pracovní úrovni třeba uzavření smluv a zakotvení vazeb přímé spolupráce na prováděcí úrovni s bezpečnostními složkami (například zpravodajské služby), prvky kritické infrastruktury a bezpečnost v oblasti informačních technologií zajišťujícími subjekty (např. právě pracoviště typu CERT/CSIRT).
- Ve všech zainteresovaných veřejných institucích je třeba vytvořit jednoznačné kontaktní body věnované tématu informační bezpečnosti a kriminality (které ob stojí při jakékoli personální turbulenci). Zainteresovaní experti z jednotlivých institucí si musí na pravidelné (případně i denní) bázi vyměňovat relevantní zkušenosti či dokonce vytvořit společný „poznatkový fond“.

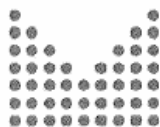
⁵⁰ KRULÍK, Oldřich. Návrhy a doporučení pro oblast informační bezpečnosti. In: Bezpečnostní situace v České republice. Ed. Marešová, Alena. Praha: odbor bezpečnostní politiky Ministerstva vnitra České republiky, 2012, CD-ROM. ISBN 978-80-260-3275-5.

HNÍK, Václav; KRULÍK, Oldřich; POŽÁR, Josef. Česká republika na rozcestí (I). Security World. 2011, č. 1, s. 44 až 47. ISSN 977-12-1479-401-6.

HNÍK, Václav; KRULÍK, Oldřich; POŽÁR, Josef. Česká republika na rozcestí (II). Security World. 2011, č. 2, s. 44 až 47. ISSN 977-12-1479-401-6.

⁵¹ Trusted Introducer for CSIRTs in Europe <<http://www.trusted-introducer.org/>>.

Příloha: Memorandum o Computer Security Incident Response Team České republiky
z prosince 2010.⁵²



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY



MEMORANDUM O COMPUTER SECURITY INCIDENT RESPONSE TEAM ČESKÉ REPUBLIKY

Česká republika – Ministerstvo vnitra

Nad Štolou 3

170 34 Praha 7

IČ 00007064

zastoupené Mgr. Radkem Johnem, ministrem vnitra České republiky

(„ministerstvo“)

a

CZ.NIC, z.s.p.o.

Americká 23

120 00 Praha 2

IČ: 67985726

zastoupené Mgr. Ondřejem Filipem, MBA, ředitelem sdružení, na základě plné moci

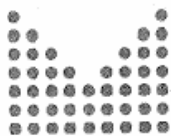
(„sdružení CZ.NIC“)

VZHLEDEM K TOMU, ŽE

- A. Ministerstvo je ústředním orgánem státní správy pro oblast informačních systémů veřejné správy a koordinátorem pro informační a komunikační technologie;
- B. Sdružení CZ.NIC je zájmovým sdružením právnických osob sdružujícím významné právnické osoby působící v České republice v oblasti doménových jmen a na trhu služeb elektronických komunikací, které spravuje národní doménu nejvyšší úrovně .cz (ccTLD .cz) a zabývá se bezpečností internetu a počítačovou bezpečností;
- C. Internet a datové sítě jsou nezbytnou součástí kritické infrastruktury státu a jejich bezpečnost je důležitá jak pro činnost veřejné správy, tak pro soukromoprávní subjekty;

⁵² Memorandum o Computer Security Incident Response Team České republiky. [cit. 6. 3. 2011]. Dostupné na World Wide Web: <http://www.nic.cz/files/nic/doc/Memorandum_CSIRT.CZ.pdf>.

CSIRT.CZ a jeho první rok fungování v roli Národního CSIRT České republiky; in: CSIRT.cz, 12. I. 2012 <<http://csirt.cz/page/992/csirt.cz--a--jeho-prvni-rok-fungovani-v-rol-i-narodniho-csirt-ceske-republiky/>>.



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY



- D. Činnost dosavadního pracoviště národního CSIRT týmu realizovaného při CESNET, z.s.p.o., končí a sdružení CZ.NIC a CESNET, z.s.p.o., se dohodly, že sdružení CZ.NIC agendu tohoto pracoviště převezme;

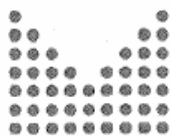
uzavírají strany níže uvedeného dne, měsíce a roku toto memorandum.

I. NÁRODNÍ CSIRT TÝM ČESKÉ REPUBLIKY

1. Ministerstvo a sdružení CZ.NIC se dohodly, že sdružení CZ.NIC převezme agendu národního „Computer Security Incident Response Team“ České republiky (dále jen „**CSIRT.CZ**“) a jeho agendu bude dále budovat a rozvíjet.
2. CSIRT.CZ se bude jako národní tým podílet na řešení incidentů týkajících se kybernetické bezpečnosti v sítích provozovaných v České republice (incident response). CSIRT.CZ bude poskytovat při řešení incidentů koordinační pomoc, nikoliv fyzickou podporu, tato pomoc přitom nebude poskytována přímo koncovým uživatelům. CSIRT.CZ bude shromažďovat a vyhodnocovat data o oznámených incidentech a předávat hlášené incidenty osobám zodpovědným za chod sítě/služby, která je zdrojem daného incidentu a to v souladu se závažností incidentu.
3. CSIRT.CZ bude plnit roli národního PoC (Point of Contact) pro oblast informačních technologií, bude centrem vzdělávání a šíření osvěty v oblasti kybernetické bezpečnosti, bude umožňovat spolupráci na národní i mezinárodní úrovni, výměnu zkušeností a informací a pomáhat se zřizováním CERT/CSIRT týmů v sítích provozovaných v České republice a pomáhat jim s navázáním spolupráce se světovými bezpečnostními platformami. Národní i mezinárodní výměna informací mezi CSIRT.CZ a dalšími CERT/CSIRT týmy bude probíhat v závislosti na jejich citlivosti a závažnosti situace v souladu s platnými právními předpisy a zvyklostmi tak, aby nedošlo k jejich zneužití.
4. CSIRT.CZ bude při své činnosti úzce spolupracovat s CSIRT týmem státní správy, do jehož působnosti budou spadat incidenty týkající se kybernetické bezpečnosti v sítích státní správy České republiky (dále jen „**vládní CSIRT**“). Do doby zřízení vládního CSIRT, nejdéle však do 30.6.2012, bude sdružení CZ.NIC plnit funkci PoC (Point of Contact) pro síť veřejné a státní správy České republiky.
5. Činnost CSIRT.CZ bude realizována v souladu s provozními dokumenty vydanými sdružením CZ.NIC na základě projednání jejich návrhů s Ministerstvem a po případných konzultacích jejich návrhů s odbornou veřejností (dále jen „**provozní dokumenty**“).

II. KONCEPČNÍ ŘÍZENÍ CSIRT.CZ

1. Činnost CSIRT.CZ bude řízena v souladu s provozními dokumenty.
2. K efektivnímu koncepčnímu řízení CSIRT.CZ mohou být ustanoveny jeden nebo více orgánů, ve kterých vedle pracovníků sdružení CZ.NIC (či CSIRT.CZ) a Ministerstva (či vládního CSIRT) mohou



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY



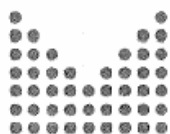
zasedat i další osoby z řad odborné veřejnosti, zástupci akademické sféry či neziskového sektoru.

III. FINANCOVÁNÍ PROVOZU CSIRT.CZ

1. Náklady spojené s provozem CSIRT.CZ ponese sdružení CZ.NIC.
2. Ministerstvo se na financování CSIRT.CZ nebude podílet. Tím však není vyloučena možnost získání grantu na provoz CSIRT.CZ, bude-li takový grant vypsán a splní-li sdružení CZ.NIC podmínky pro jeho přidělení.
3. Ministerstvo bude podporovat sdružení CZ.NIC v případě, že financování CSIRT.CZ bude možné získat nebo podpořit z fondů Evropské Unie či mezinárodních organizací.

IV. PRÁVA A POVINNOSTI SDRUŽENÍ CZ.NIC

1. Sdružení CZ.NIC deklaruje, že disponuje dostatečnými technickými a personálními zdroji nezbytnými k bezproblémovému provozu CSIRT.CZ, a to jak v rámci České republiky, tak pro účely spolupráce a koordinace na mezinárodní úrovni.
2. Sdružení CZ.NIC zahájí nejpozději od 1.1.2011 přebírání provozu dosavadního modelového pracoviště národního CSIRT provozovaného sdružením CESNET, z.s.p.o., a do pěti měsíců ode dne podpisu tohoto memoranda zahájí plný technický provoz CSIRT.CZ, a to za předpokladu, že sdružení CESNET, z.s.p.o., zahájí bezodkladně předávání agendy tohoto pracoviště sdružení CZ.NIC. V případě, že sdružení CESNET, z.s.p.o. předávání agendy zahájí, zabezpečí sdružení CZ.NIC funkcionality CSIRT.CZ po dobu předávání na stejné úrovni na jaké ji v současné době provozuje sdružení CESNET, z.s.p.o. Sdružení CZ.NIC následně zabezpečí plnou funkcionality CSIRT.CZ v rozsahu uvedeném v tomto memorandu, včetně všech nezbytných akreditací, nejpozději do dvanácti měsíců od zahájení jeho technického provozu.
3. V případě, že se v průběhu řešení některého z incidentů CSIRT.CZ objeví situace, která má nebo může mít významný bezpečnostní dopad na síť státní správy (informace o řízeném útoku apod.) je sdružení CZ.NIC povinno tuto informaci neprodleně postoupit vládnímu CSIRT, do doby jeho uvedení do provozu pak odboru kybernetické a informační bezpečnosti MVČR případně složkám dle eskalačních procedur odzkoušených a používaných v současné době sdružením CESNET, z.s.p.o.. Detailně bude tato komunikace a následné řešení incidentů definováno v provozních dokumentech.
4. Sdružení CZ.NIC je povinno postupovat v souladu s pokyny Ministerstva či vládního CSIRT v případě, že tuto spolupráci vyžadují okolnosti, které mají významný dopad na kybernetickou bezpečnost České republiky. Zároveň má povinnost zúčastnit se na požádání Ministerstva mezinárodních cvičení a případných dalších akcí, souvisejících s provozem CSIRT.CZ.
5. Sdružení CZ.NIC má povinnost zveřejňovat pravidelné zprávy o činnosti CSIRT.CZ, a to nejméně jednou ročně. Před zveřejněním zprávy předloží sdružení CZ.NIC zprávu k připomínkám Ministerstvu.



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY



V. PODPORA MINISTERSTVA

1. Ministerstvo řeší postavení pracovišť typu CSIRT v rámci státní správy v českém právním řádu. Ministerstvo dále bude podporovat zařazení CSIRT.CZ do mezinárodních struktur, a to zejména tím, že potvrdí statut CSIRT.CZ jako národního CSIRT týmu.
2. Ministerstvo připomínkuje provozní dokumenty CSIRT.CZ a zprávy o činnosti CSIRT.CZ, předkládané sdružením CZ.NIC.
3. Ministerstvo má právo požádat o provedení auditu výkonu činnosti CSIRT.CZ. V takovém případě sdružení CZ.NIC audit provede a s jeho výsledkem seznámí Ministerstvo.
4. Ministerstvo vyhodnocuje informace, které obdrží od CSIRT.CZ v případě, že CSIRT.CZ má podezření, že řešený incident může mít dopad na systémy státu, resp. státní správy.
5. Ministerstvo koordinuje činnost CSIRT.CZ a vládního CSIRT.
6. Ministerstvo se zavazuje využít svých pravomocí v systému krizových opatření (zákon č. 240/2000 Sb.) k tomu, aby umožnilo sdružení CZ.NIC řádně provozovat CSIRT.CZ v souladu s tímto memorandem.

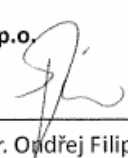
VI. RŮZNÉ

1. Každá ze stran je oprávněna toto memorandum vypovědět v případě změny okolností vzájemné spolupráce tak, jak je popsána v tomto memorandu, s nimiž strana nebude souhlasit. V takovém případě jsou strany povinny udělat ve vzájemné spolupráci takové nezbytné kroky, aby agenda CSIRT.CZ mohla být bez zbytečného odkladu předána novému provozovateli.
2. Strany se zavazují informovat se navzájem o svých postojích k otázkám týkajícím se jejich činnosti dle tohoto memoranda a konzultovat vzniklé problémy. Za tímto účelem každá ze stran označí osobu, která bude vůči druhé straně kontaktním místem.
3. Strany budou spolupracovat na přípravě a zveřejnění společné tiskové zprávy s cílem zajistit pozitivní publicitu jejich spolupráce. Strany jsou oprávněny zveřejnit plný text memoranda.
4. Obě strany souhlasí tím, že každá z nich ponese své vlastní náklady spojené s realizací cílů uvedených v memorandu.
5. Podpisem tohoto memoranda nemají strany v úmyslu vytvářet vůči sobě žádný jiný právní závazek, než jaký vyplývá z jejich vzájemného prohlášení o způsobu spolupráce ve zde uvedených oblastech.

Česká republika - Ministerstvo vnitra

Podpis: 
Jméno: Mgr. Radek John
Funkce: Ministr vnitra
Datum: 9. 12. 2010

CZ.NIC, z.s.p.o.

Podpis: 
Jméno: Mgr. Oldřej Filip, MBA
Funkce: ředitel sdružení
Datum: 30. 11. 2010

Příloha: Nové memorandum uzavřené v prosinci 2012 mezi CZ.NIC a Národním bezpečnostním úřadem (vstoupilo v platnost 1. ledna 2013 a bude platit po dobu tří let).⁵³

MEMORANDUM

O

COMPUTER EMERGENCY RESPONSE TEAM / COMPUTER SECURITY INCIDENT RESPONSE TEAM ČESKÉ REPUBLIKY

Česká republika – Národní bezpečnostní úřad

Na Popelce 2/16

150 06 Praha 5

IČ: 68403569

zastoupené Ing. Dušanem Navrátillem, ředitelem Národního bezpečnostního úřadu („NBÚ“)

a

CZ.NIC, z.s.p.o.

Americká 23

120 00 Praha 2

IČ: 67985726

zastoupené Mgr. Ondřejem Filipem, MBA, ředitelem sdružení, na základě plné moci („sdružení CZ.NIC“)

VZHLEDEM K TOMU, ŽE

- A. NBÚ je na základě usnesení vlády České republiky ze dne 19. října 2011 č. 781 gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast;
- B. Sdružení CZ.NIC je zájmovým sdružením právnických osob sdružujícím významné právnické osoby působící v České republice v oblasti doménových jmen a na trhu služeb elektronických komunikací, které spravuje národní doménu nejvyšší úrovně .cz (ccTLD .cz) a zabývá se bezpečností internetu a počítačovou bezpečností;
- C. Internet a datové sítě jsou nezbytnou součástí kritické infrastruktury státu a jejich bezpečnost je důležitá jak pro činnost veřejné správy, tak pro soukromoprávní subjekty;

uzavírají strany níže uvedeného dne, měsíce a roku toto memorandum.

strana 1

⁵³ CZ.NIC a Národní bezpečnostní úřad podepsali nové memorandum o spolupráci; in: CZ.NIC, 19. XII. 2012 <<http://www.nic.cz/page/1308/cz.nic-a-nbu-podepsali-nove-memorandum-o-spolupraci/>>.

MEMORANDUM

I. NÁRODNÍ CSIRT TÝM ČESKÉ REPUBLIKY

1. NBÚ a sdružení CZ.NIC se dohodly, že sdružení CZ.NIC bude dále budovat a rozvíjet agendu národního „Computer Security Incident Response Team“ České republiky (dále jen „CSIRT.CZ“).
2. CSIRT.CZ se bude jako národní tým podílet na řešení incidentů týkajících se kybernetické bezpečnosti v sítích provozovaných v České republice (incident response). CSIRT.CZ bude poskytovat při řešení incidentů koordinační a metodickou pomoc, nikoliv fyzickou podporu. CSIRT.CZ nemá povinnost poskytovat podporu a pomoc koncovým uživatelům. CSIRT.CZ bude shromažďovat a vyhodnocovat data o oznámených incidentech a předávat hlášené incidenty osobám zodpovědným za chod sítě/služby, která je zdrojem daného incidentu a to v souladu se závažností incidentu.
3. CSIRT.CZ bude plnit roli národního PoC (Point of Contact) pro oblast informačních technologií, bude centrem vzdělávání a šíření osvěty v oblasti kybernetické bezpečnosti, bude umožňovat spolupráci na národní i mezinárodní úrovni, výměnu zkušeností a informací a pomáhat se zřizováním CERT/CSIRT týmů v sítích provozovaných v České republice a pomáhat jim s navázáním spolupráce se světovými bezpečnostními platformami. Národní i mezinárodní výměna informací mezi CSIRT.CZ a dalšími CERT/CSIRT týmy bude probíhat v závislosti na jejich citlivosti a závažnosti situace v souladu s platnými právními předpisy a zvyklostmi tak, aby nedošlo k jejich zneužití.
4. CSIRT.CZ bude při své činnosti úzce spolupracovat s CERT/CSIRT týmem státní správy zřízeným v rámci NBÚ, do jehož působnosti budou spadat incidenty týkající se kybernetické bezpečnosti v sítích státní správy a kritické informační infrastruktury České republiky (dále jen „vládní CERT“).
5. Činnost CSIRT.CZ bude realizována v souladu s provozními dokumenty vydanými sdružením CZ.NIC na základě projednání jejich návrhů s NBÚ a po případných konzultacích jejich návrhů s odbornou veřejností (dále jen „provozní dokumenty“). Kopie provozních dokumentů v aktuálním znění je uložena u NBÚ.
6. Sdružení CZ.NIC deklaruje, že disponuje dostatečnými technickými a personálními zdroji nezbytnými k bezproblémovému provozu CSIRT.CZ, a to jak v rámci České republiky, tak pro účely spolupráce a koordinace na mezinárodní úrovni.
7. Sdružení CZ.NIC zabezpečí plný technický provoz a plnou funkcionalitu CSIRT.CZ v rozsahu uvedeném v tomto memorandu, včetně všech nezbytných akreditací.

II. KONCEPČNÍ ŘÍZENÍ CSIRT.CZ

1. Činnost CSIRT.CZ bude řízena v souladu s provozními dokumenty.
2. K efektivnímu koncepčnímu řízení CSIRT.CZ mohou být ustanoveny jeden nebo více orgánů, ve kterých vedle pracovníků sdružení CZ.NIC (CSIRT.CZ) a NBÚ (vládní CERT) mohou zasedat i další osoby z řad odborné veřejnosti, zástupci akademické sféry či neziskového sektoru.

MEMORANDUM

III. FINANCOVÁNÍ PROVOZU CSIRT.CZ

1. Náklady spojené s provozem CSIRT.CZ ponese sdružení CZ.NIC. NBÚ se na financování CSIRT.CZ nebude podílet.
2. Sdružení CZ.NIC může získat podporu financování provozu CSIRT.CZ ze soukromých, resortních, vládních, či mezinárodních zdrojů, a to zejména formou grantů či čerpání fondů.
3. NBÚ bude podporovat sdružení CZ.NIC při případném získávání financování provozu CSIRT.CZ, pokud to nebude možné považovat za střet zájmů vzhledem k zapojení NBÚ v orgánech, které budou o poskytnutí financování rozhodovat.

IV. VZÁJEMNÁ SPOLUPRÁCE V OBLASTI KYBERNETICKÉ BEZPEČNOSTI

1. Zájemem obou stran je úzká spolupráce v oblasti kybernetické bezpečnosti, a to v rámci působnosti CSIRT.CZ a vládního CERT.
2. Sdružení CZ.NIC (CSIRT.CZ) a NBÚ (vládní CERT) budou úzce spolupracovat na rozvoji a dalším vývoji schopností obou vrcholových pracovišť tak, aby byla zachována jejich kompatibilita a zlepšovány jejich schopnosti efektivní a účinné ochrany kyberprostoru České republiky, a to zejména konzultacemi při budování CSIRT.CZ a vládního CERT, vzájemnou podporou a poskytováním informací. Výsledky výzkumných úkolů a řešení budou poskytnuty pro využití všemi subjekty spolupracujícími na ochraně kybernetického prostoru, včetně orgánů veřejné správy a subjektů kritické informační infrastruktury. V počátečních fázích fungování odborného pracoviště NBÚ (vládní CERT) CZ.NIC (CSIRT.CZ) pomáhá NBÚ s jeho výstavbou a zařazením do mezinárodních struktur.
3. Sdružení CZ.NIC (CSIRT.CZ) a NBÚ (vládní CERT) budou úzce spolupracovat na osvětě v oblasti kybernetické bezpečnosti v České republice formou pořádání seminářů, přednášek, konferencí, školení, účasti na akcích týkajících se této oblasti a vydáváním materiálů k tomuto tématu v elektronické i tištěné podobě. Obě strany se budou navzájem v dostatečném předstihu informovat o těchto připravovaných aktivitách, budou koordinovat jejich přípravu, aby nedocházelo ke zbytečnému překrývání a budou si navzájem poskytovat prostor pro účast v těchto aktivitách, např. formou přednáškové činnosti apod. Osvěta v oblasti kybernetické bezpečnosti bude dle možností obou stran zahrnovat všechny dotčené subjekty včetně subjektů veřejné správy a kritické informační infrastruktury.
4. Sdružení CZ.NIC bude aktivně podporovat vznik nových bezpečnostních týmů u subjektů státní správy, kritické infrastruktury, akademických institucí i soukromých společností.
5. V případě, že se v průběhu řešení některého z incidentů CSIRT.CZ objeví situace, která má nebo může mít významný bezpečnostní dopad na síť státní správy nebo kritické informační infrastruktury (informace o řízeném útoku apod.) sdružení CZ.NIC tuto informaci neprodleně postoupí NBÚ (vládnímu CERT) a dále bude při řešení incidentu postupovat v koordinaci s ním.

MEMORANDUM

6. Sdružení CZ.NIC bude postupovat v souladu s pokyny NBÚ (vládního CERT) v případě, že tuto spolupráci vyžadují okolnosti, které mají významný dopad na kybernetickou bezpečnost České republiky. Zároveň se na požádání NBÚ zúčastní mezinárodních cvičení a případných dalších akcí, souvisejících s provozem CSIRT.CZ a kybernetickou bezpečností České republiky.
7. Sdružení CZ.NIC se bude podílet na tvorbě a budoucích změnách legislativy a dalších návazných dokumentů a předpisů v oblasti kybernetické bezpečnosti. NBÚ bude se sdružením CZ.NIC konzultovat tvorbu legislativy a uvedených dokumentů a předpisů.
8. Sdružení CZ.NIC (CSIRT.CZ) se bude na základě oslovení NBÚ účastnit zasedání krizového štábu při řešení závažných bezpečnostních incidentů, které mohou mít významný bezpečnostní dopad na síť státní správy a kritické informační infrastruktury. Sdružení CZ.NIC poskytne NBÚ kontaktní údaje na osoby, které budou tuto povinnost sdružení CZ.NIC plnit, a které splňují podmínky pro přístup k případným utajovaným informacím, se kterými mohou být v této souvislosti seznámeny, a to přinejmenším pro stupeň utajení „Vyhrazené“.
9. NBÚ řeší postavení pracovišť typu CERT/CSIRT v českém právním řádu. NBÚ dále bude podporovat zařazení CSIRT.CZ do mezinárodních struktur, a to zejména tím, že potvrdí statut CSIRT.CZ jako národního CSIRT týmu.
10. NBÚ připomínkuje provozní dokumenty CSIRT.CZ a zprávy o činnosti CSIRT.CZ, předkládané sdružením CZ.NIC.
11. NBÚ má právo požádat o provedení auditu výkonu činnosti CSIRT.CZ. V takovém případě sdružení CZ.NIC audit provede a jeho výsledek předloží NBÚ.
12. NBÚ vyhodnocuje informace, které obdrží od CSIRT.CZ v případě, že CSIRT.CZ má podezření, že řešený incident může mít dopad na systémy státu, resp. státní správy a kritické informační infrastruktury.
13. NBÚ koordinuje činnost CSIRT.CZ a vládního CERT.
14. NBÚ předkládá každoročně zprávu o činnosti CSIRT/CERT v České republice evropské agentuře ENISA.

V. INFORMAČNÍ ČINNOST

1. Sdružení CZ.NIC (CSIRT.CZ) bude na svých stránkách průběžně zveřejňovat aktualizované informace a statistiky o počtu a druhu řešených incidentů. Na vyžádání NBÚ (vládního CERT) sdružení CZ.NIC předloží o těchto incidentech detailnější informace.
2. Sdružení CZ.NIC bude zveřejňovat pravidelné zprávy o činnosti CSIRT.CZ, a to nejméně jednou ročně. Před zveřejněním zprávy předloží sdružení CZ.NIC zprávu k připomínkám NBÚ. Informace ze zprávy budou jedním z podkladů pro tvorbu společné zprávy o stavu kybernetické bezpečnosti v České republice předkládané vládě ČR 1x ročně. Při přípravě společné zprávy o stavu kybernetické bezpečnosti v České republice předkládané vládě ČR budou obě strany spolupracovat. CZ.NIC rovněž bude NBÚ poskytovat podklady pro

MEMORANDUM

vypracování společné zprávy o činnosti CSIRT/CERT v České republice pro příslušnou evropskou agenturu. Tuto zprávu bude NBÚ evropské agentuře předkládat počínaje zprávou za rok 2013.

3. Strany budou spolupracovat na přípravě a zveřejnění společné tiskové zprávy s cílem zajistit pozitivní publicitu jejich spolupráce. Strany jsou oprávněny zveřejnit plný text memoranda.

VI. RŮZNÉ

1. Toto memorandum nabývá, po dohodě obou smluvních stran, účinnosti dnem 1. 1. 2013 a pozbývá platnosti dne 31. 12. 2015. Strany shodně prohlašují, že do data pozbytí účinnosti tohoto memoranda vyvinou úsilí k tomu, aby uzavřely obdobný dokument, jehož předmětem bude provozování agendy CSIRT.CZ. Obě strany se zavazují informovat se navzájem v dostatečném předstihu před uplynutím doby, na kterou je toto memorandum sjednáváno, nejméně však 3 měsíce předem, pokud nehodlají takový dokument pro období po ukončení účinnosti tohoto memoranda uzavřít.
2. Každá ze stran je oprávněna toto memorandum vypovědět i před datem 31. 12. 2015 v případě změny okolností a neplnění podmínek vzájemné spolupráce tak, jak je popsána v tomto memorandu, a to s výpovědní lhůtou 3 měsíců. Každá ze stran je rovněž oprávněna toto memorandum vypovědět i bez uvedení důvodu s výpovědní lhůtou 9 měsíců. V případě výpovědi jsou strany povinny udělat ve vzájemné spolupráci takové nezbytné kroky, aby agenda CSIRT.CZ mohla být bez zbytečného odkladu předána novému provozovateli.
3. Strany se zavazují informovat se navzájem o svých postojích k otázkám týkajícím se jejich činnosti podle tohoto memoranda a konzultovat vzniklé problémy. Za tímto účelem každá ze stran označí osobu, která bude vůči druhé straně kontaktním místem.
4. Obě strany souhlasí tím, že každá z nich ponese své vlastní náklady spojené s realizací cílů uvedených v memorandu.
5. Podpisem tohoto memoranda nemají strany v úmyslu vytvářet vůči sobě žádný jiný právní závazek, než jaký vyplývá z jejich vzájemného prohlášení o způsobu spolupráce ve zde uvedených oblastech.
6. Obě strany se zavazují zachovávat mlčenlivost o skutečnostech, které druhá strana označí jako důvěrné informace (tedy nikoli utajované podle zvláštních právních předpisů), nebo které představují utajované informace podle právních předpisů. Povinnost mlčenlivosti se nevztahuje na uveřejňování statistik a základních informací o bezpečnostních incidentech. Povinnost mlčenlivosti trvá i po skončení účinnosti memoranda. Za porušení povinnosti mlčenlivosti se nepovažuje, je-li strana povinna informaci sdělit na základě zákonem stanovené povinnosti.
7. Tímto memorandem se ruší a v celém rozsahu nahrazuje Memorandum uzavřené mezi stranami dne 28.3.2012.

MEMORANDUM

Česká republika – Národní bezpečnostní úřad

CZ.NIC, z.s.p.o.

Podpis:

Jméno: Ing. Dušan Navrátil

Funkce: ředitel Národního bezpečnostního úřadu

Datum: 19. 12. 2012

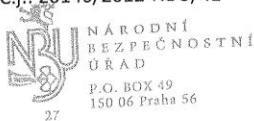
Podpis:

Jméno: Mgr. Ondřej Filip, MBA

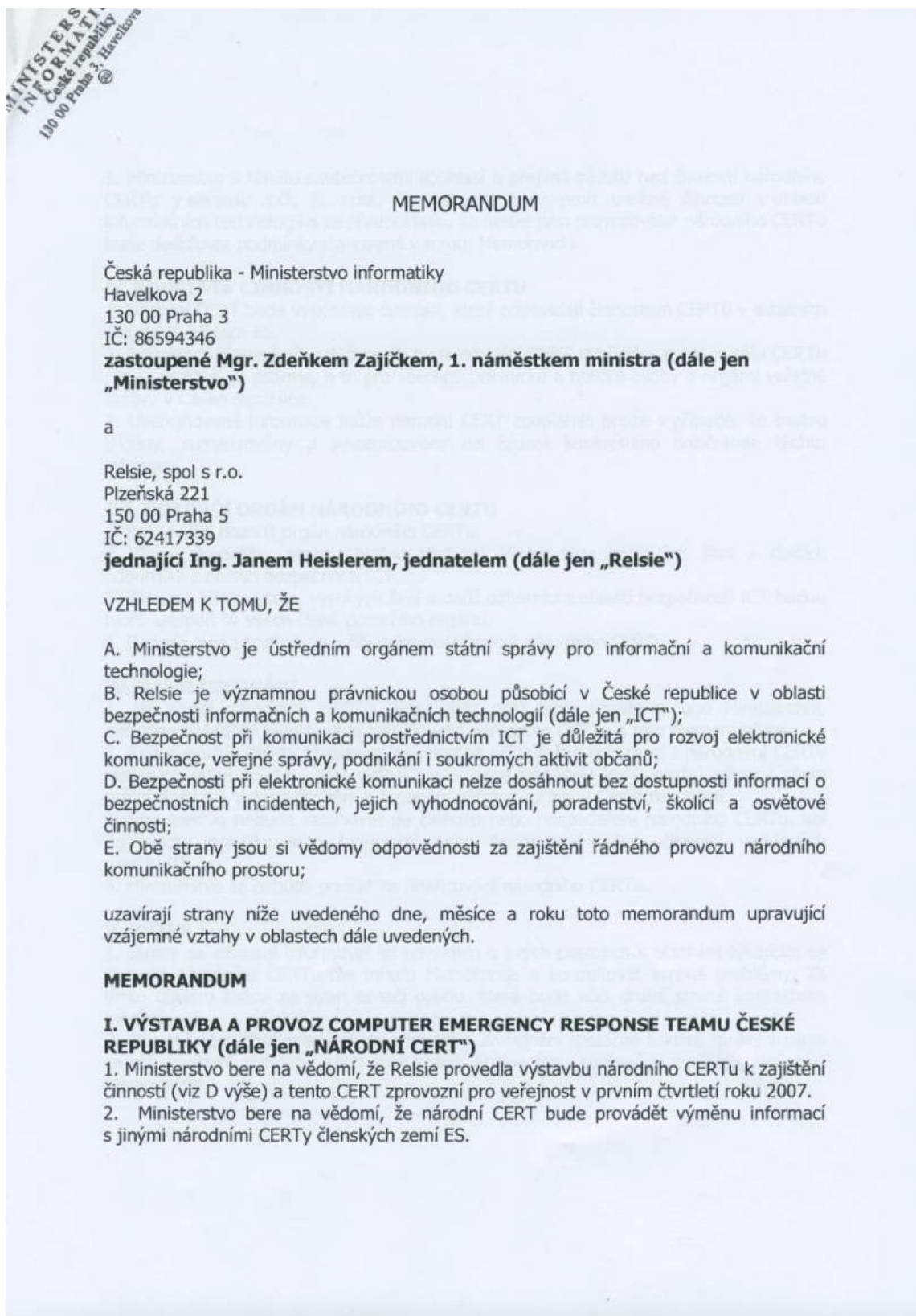
Funkce: ředitel sdružení

Datum: 19. 12. 2012

Č.j.: 20140/2012-NBÚ/41



Příloha: Memorandum mezi firmou RELSIE a Ministerstvem vnitra z února 2007.



3. Ministerstvo s těmito skutečnostmi souhlasí a přejímá záštitu nad činností národního CERTu v souladu s čl. B, odst. 7 Koncepce boje proti trestné činnosti v oblasti informačních technologií a za předpokladu, že Relsie jako provozovatel národního CERTu bude dodržovat podmínky stanovené v tomto Memorandu.

II. PODSTATA ČINNOSTI NÁRODNÍHO CERTU

1. Národní CERT bude vykonávat činnosti, které odpovídají činnostem CERTů v ostatních členských státech ES.
2. Informace získané při své činnosti bude národní CERT uveřejňovat na portálu CERTu (www.certcz.org) zdarma, a to pro všechny právnické a fyzické osoby a orgány veřejné správy v České republice.
3. Uveřejňované informace může národní CERT zpoplatnit pouze v případě, že budou tříděny, sumarizovány a systemizovány na žádost konkrétního odběratele těchto informací.

III. DOZORČÍ ORGÁN NÁRODNÍHO CERTU

1. Relsie zřídí dozorčí orgán národního CERTu.
2. Členy dozorčího orgánu budou zástupci Ministerstva, vysokých škol a dalších odborníků z oblasti bezpečnosti ICT.
3. Zástupci Ministerstva, vysokých škol a další odborníci z oblasti bezpečnosti ICT budou tvořit alespoň ¾ všech členů dozorčího orgánu.
4. Dozorčí orgán kontroluje a řídí odbornou činnost národního CERTu.

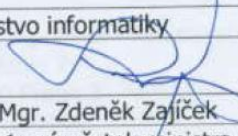
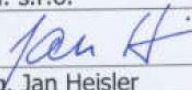
IV. DALŠÍ UJEDNÁNÍ

1. Na portál národního CERTu (www.certcz.org) bude umístěno logo Ministerstva, informace o záštitě Ministerstva nad činností národního CERTu a toto memorandum.
2. Relsie využije záštitu Ministerstva výhradně při výměně informací s národními CERTy členských zemí ES tak, aby získané informace přinášely konkurenční výhody všem právnickým a fyzickým osobám a orgánům veřejné správy v České republice.
3. Ministerstvo nebude zasahovat do činnosti nebo hospodaření národního CERTu, ani do tvorby pravidel jeho fungování nebo financování vyjma činností uvedených v bodu III.
4. Ministerstvo se nebude podílet na financování národního CERTu.

V. RŮZNÉ

1. Strany se zavazují informovat se navzájem o svých postojích k otázkám týkajícím se činnosti národního CERTu dle tohoto Memoranda a konzultovat vzniklé problémy. Za tímto účelem každá ze stran označí osobu, která bude vůči druhé straně kontaktním místem.
2. Strany budou spolupracovat na přípravě a zveřejnění společné tiskové zprávy s cílem zajistit pozitivní publicitu jejich spolupráce. Strany jsou oprávněny zveřejnit plný text Memoranda.

3. Podpisem Memoranda nemají strany v úmyslu vytvářet vůči sobě žádný jiný právní závazek, než jaký vyplývá z jejich vzájemného prohlášení o způsobu spolupráce ve zde uvedených oblastech.

Ministerstvo informatiky	Relsie, spol. s r.o.
Podpis: 	Podpis: 
Jméno: Mgr. Zdeněk Zajíček	Jméno: Ing. Jan Heisler
Funkce: 1. náměstek ministra	Funkce: jednatel společnosti
Datum: 1.2.2007	Datum: - 1 -02- 2007

Relsie, spol. s r.o.

Přízeňská 221, 150 00 PRAHA 5
sídlí: Na Stárce 12, 150 00 PRAHA 5
www.relsie.cz • DIČ: CZ62417339

Relsie, spol. s r.o.

Přízeňská 221

150 00 PRAHA 5

DIČ: CZ62417339

Jednatel Ing. Jan Heisler, jednatel (jméno Jan „Relsie“)

ZNALESTI K TOMU ŽE:

A. Informace je každá informace, která je v rámci své podstaty a charakteru technická.

B. Informace je každá informace, která je v rámci své podstaty a charakteru technická a která je v rámci své podstaty a charakteru technická.

C. Informace je každá informace, která je v rámci své podstaty a charakteru technická a která je v rámci své podstaty a charakteru technická.

D. Informace je každá informace, která je v rámci své podstaty a charakteru technická a která je v rámci své podstaty a charakteru technická.

E. Informace je každá informace, která je v rámci své podstaty a charakteru technická a která je v rámci své podstaty a charakteru technická.

F. Informace je každá informace, která je v rámci své podstaty a charakteru technická a která je v rámci své podstaty a charakteru technická.

MEMORANDUM

1. VYSTAVBA A PRÁCE COMPUTER EMERGENCY RESPONSE TEAMU ČESKÉ REPUBLIKY (Jméno Jan „Relsie“ CERT)

2. Memorandum bylo vypracováno v rámci projektu „Vytváření CERTu v ČR“ a bylo vypracováno v rámci projektu „Vytváření CERTu v ČR“.

3. Memorandum bylo vypracováno v rámci projektu „Vytváření CERTu v ČR“ a bylo vypracováno v rámci projektu „Vytváření CERTu v ČR“.

Příloha: „Retrospektivní“ přehled, připravený v průběhu roku 2008 (autoři Oldřich Krulík a Václav Hník): Pracoviště typu CERT/CSIRT, srovnání situace v některých zemích světa (Ministerstvo vnitra, odbor bezpečnostní politiky, příloha č. 1 k č. j.: MV-1752/OBP-K-2008).

země	počet členů akreditovaných v ENISA	počet členů akreditovaných ve FIRST	existuje zde národní CERT	jaká instituce jej provozuje	poznámka	spolupráce s firmou Microsoft ⁵⁴	napojení na CETS Microsoft
Belgie	2	2	ano (BELNET, od roku 2004)	univerzitní pracoviště, veřejná správa a výzkumné ústavy	vedle toho v Belgii existuje CERT pro vojenské účely (NCIRC), vybudovaný roku 2004 a používaný strukturou celé Severoatlantické aliance	stránka BELNET o operačním systému Windows vůbec nehovoří, obsahuje jen odkazy na systémy LINUX, SOLARIS, HP-UX a APPLE; uživatelé produktů Microsoft odkazují pouze na stránky této firmy ⁵⁵ ; firma Microsoft o přímou spolupráci opakovaně usilovala, ale zřejmě bez výsledku	ne
Bulharsko	0	0	ne	-	-	nepodařilo se zjistit	připravuje se
Česká republika	1 (CESNET)	0	ne	-	akademické pracoviště CERT je jediným certifikovaným pracovištěm v ČR, v oblasti bezpečnostních incidentů komunikuje s TF CERT a FIRST;	základem spolupráce je dohoda z února 2005 mezi firmou Microsoft a Národním bezpečnostním úřadem; pracoviště CESNET se případné spolupráci nebrání	ne, téma spadá do působnosti Policie České republiky
Dánsko	3	6	ano (DK-CERT, od roku 1991, po USA jeden z prvních CERT světa)	výzkumné a vzdělávací instituce, platforma, provozující CERT je nyní přidruženou agenturou Státního střediska pro výzkum v oblasti informačních technologií, financovanou Ministerstvem vzdělávání	vedle toho v zemi existuje dalších 5 omezenějších pracovišť podobného typu (CSIRT od roku 1999, vybudovaný komerčními internetovými a telekomunikačními operátory; KMD, vybudovaný rok 1997 pro účely místních úřadů, NORDUNET z roku 2002, SWAT a SECUNIA RESEARCH.	-	ne
Estonsko	1	0	ano (CERT-EE, od roku 2006)	subjekty veřejného a soukromého sektoru (vládním subjektům je v platformě určeno zvláštní „podokno“)	-	stránka CERT-EE o produktech Microsoft de facto vůbec nehovoří a ani na ně neodkazuje	ne
Finsko	4	5	ano (CERT-FI, od roku 2002)	vládní subjekty, telekomunikační operátoři, vlastníci přenosových soustav	v zemi existuje ještě čtyři soukromé platformy: PSIRT Ericsson (založen roku 2000); NIRT Nokia (založeno 1998), FUNET (od roku 1995) a FS-Laboratories (od roku 1991)	-	ne
Francie	4	3	ano (RENATER, od roku 1993)	ústřední orgány státní správy, výzkumná pracoviště	struktura CERTA, určená pro potřeby veřejné správy v území (obce, regiony), fungující od roku 1999 a dvě soukromé platformy CERT-IST (od roku 1999) a LEXSI (od roku 2003)	-	ne

⁵⁴ Pokud není uvedeno jinak, pracoviště standardně upozorňuje na incidenty a bezpečnostní inovace, související s produkty firmy Microsoft, stránka ale neobsahuje její logo a nehovoří o nějakých nadstandardních vztazích.

⁵⁵ <http://www.microsoft.com/security/default.msp>

Kypr	1	0	ne	-	v zemi existuje jen akademická platforma CYNET (od roku 2001)	nepodařilo se zjistit, stránka je pouze v řečtině	ne
Chorvatsko	1	1	ano (CARNET od roku 1996)	akademické subjekty, operátoři, správci domén	-	výstrahy jsou vždy specifikovány podle toho, jakého operačního systému se týkají (UNIX, LINUX, WINDOWS, ostatní), pracoviště standardně upozorňuje na bezpečnostní inovace, související s produkty firmy Microsoft, stránka ale neobsahuje její logo a nehovoří o nějakých nadstandardních vztazích	ne
Irsko	1	0	ne	-	v zemi působí pouze omezenější platforma HEANET (CERT-IE), od roku 2002, pokrývají síť akademických institucí		ne
Island	1	0	ne	-	v zemi pouze existuje akademická platforma RHNET (od roku 2003)	nepodařilo se s určitostí zjistit (většina textu je v islandštině); firma Microsoft patrně uzavřela smlouvy s universitami, které RHNET provozují (slevy na produkty pro pedagogy i studenty), ale nikoli s platformou RHNET jako takovou	ne
Itálie	8	1	ano (CERT-IT, od roku 1994)	Universita Miláno a operátoři	vedle toho existuje ještě vládní platforma GOVCERT pro potřeby veřejné sféry, struktura DIFESA pro potřeby armády a pět dalších (akademické, soukromé) subjektů tohoto typu	nepodařilo se s určitostí zjistit (stránky jsou značně neupřádané); za zmínku stojí skutečnost, že některé regionální správy (prefektury, provincie) přešly na LINUX	ano (říjen 2006)
Litva	2	1	ano (LITNET, od roku 1998)	vysoké školy, výzkumné ústavy, nevládní organizace ⁵⁶	v zemi navíc od roku 2006 funguje platforma RRT, sloužící potřebám telekomunikačních operátorů	nepodařilo se s určitostí zjistit (informace jsou pouze v litevštině)	ne
Lotyšsko	2	0	ano (LATNET od roku 2006)	akademické a soukromé subjekty	v zemi navíc od roku 2007 funguje platforma DDIRV, sloužící potřebám vládních institucí, včetně armády	LATNET o produktech Microsoft vůbec neinformuje; DDIRV jen velmi sporadicky, spíše v dílčích anketách, nikoli co se týče konkrétních incidentů	ne
Lucembur-sko	1	0	nepodařilo se zjistit s jistotou	patrně akademická pracoviště	-		ne

⁵⁶ Ministerstvo zahraničních věcí, odbor bezpečnostní politiky, č. j.: 124015/2006-OBP, 31. VII. 2006; Pospíšilová, M., Velvyslanectví České republiky v Litvě, Vilnius, 18. VIII. 2006 (č. j. 999/2006 – Vilnius); National contributions to be taken into account in the preparation of the independent report on the use of the Internet for terrorist purposes and cyberterrorism; CODEXTER (2006) 38 prov, 3. X. 2006.

Maďarsko	3	1	ano (HUN-CERT, od roku 2003)	členové asociace poskytovatelů telekomunikačních služeb	v zemi existuje dvě další platformy: CERT-HU (funguje od roku 2004, pro potřeby veřejné správy, provozovaný obdobou Národního bezpečnostního úřadu) a NIIF (od roku 2003, pro potřeby některých akademických subjektů)		ne
Malta	1	0	ano (MTCERT, od roku 2002)	orgány státní správy	-		ne
Německo	19	16	ano (CERT-BUND, od roku 2001)	Spolkový úřad pro bezpečnost informační techniky (BSI, vládní agentura)	vedle toho existuje vojenská platforma CERT-Bundeswehr (od roku 2003) a sedmnáct dalších institucí typu CERT s omezenějším záběrem (soukromé firmy, banky atd.)	CERT-BUND standardně upozorňuje na incidenty a bezpečnostní inovace, související s produkty firmy Microsoft, stránka ale neobsahuje její logo a nehovoří o nějakých nadstandardních vztazích; státní správa v Německu od roku 2002 plošně přešla na LINUX, ⁵⁷ ale firma Microsoft státní správě dále dodává celou řadu dalších aplikací ⁵⁸	ne
Nizozemsko	10	5	tuto roli patrně splňuje GOVCERT (založený roku 2002)	vládní a veřejné subjekty	vedle toho v zemi existuje dalších 9 subjektů, plnících funkci CERT pro určité úzce specifikované klienty (banky, zdravotnická zařízení, operátory, university, zákazníci soukromých firem)	o produktech firmy a incidentech, které s nimi souvisí, je informováno jen velmi sporadicky, spíše v oblasti všeobecných rad a odkazů na stránky firmy	ne
Norsko	2	2	ano (NORCERT od roku 2004)	státní subjekty, operátoři, majitelé přenosových soustav	vedle toho v zemi existuje akademická síť UNINETT (od roku 1995)	o produktech firmy a incidentech, které s nimi souvisí, je informováno jen velmi sporadicky, spíše v oblasti všeobecných rad a odkazů na stránky firmy	ne
Polsko	3	1	ano (CERT POLSKA, od roku 1996)	hlavním subjektem, který v Polsku provozuje CERT, jsou správci tzv. Vzdělávací a akademické počítačové sítě (Naukowa i Akademicka Sieć Komputerowa, NASK); jedná se o akademické pracoviště, které začalo se zaváděním Internetu v Polsku	vedle toho v zemi existují dvě omezené CERT sítě na akademické půdě (PIONEER a TPCERT, vybudované obě na přelomu let 2001 a 2002), pokrývající jen sítě konkrétních akademických pracovišť		připravuje se

⁵⁷ http://www.theregister.co.uk/2002/06/04/german_gov_deal_offers_linux/

<http://www.heise.de/english/newsticker/news/25006>

⁵⁸ <http://www.microsoft.com/presspass/press/2004/may04/05-03germanymoupr.msp>

Portugalsko	2	0	ne	-	v zemi fungují pouze dvě omezené akademické platformy (CERT-PT z roku 2002 a FEUP z roku 2006)		ne
Rakousko	1	1	ne	-	v zemi funguje (od roku 2003) pouze akademická síť ACONET	o produktech firmy a incidentech, které s nimi souvisí, je informováno jen velmi sporadicky, spíše v oblasti všeobecných rad	ne
Rumunsko	0	0	ne ⁵⁹	-	-	-	ano (od října 2007) ⁶⁰
Řecko	2	0	ne	-	v zemi existují dvě omezené CERT sítě na akademické půdě (GRNET z roku 2000 a AUTH z roku 2004), pokrývající jen sítě konkrétních akademických pracovišť	pracoviště GRNET standardně upozorňuje na incidenty a bezpečnostní inovace, související s produkty firmy Microsoft, stránka ale neobsahuje její logo a nehovoří o nějakých nadstandardních vztazích	ne
Slovensko	0	0	ne	-	-	-	ne
Slovinsko	1	1	ano (SI-CERT, od roku 1994)	akademická obec (Akademická a výzkumná síť Slovinska - Akademska in Raziskovalna Mreža Slovenije, ARNES) ⁶¹	-		ne
Spojené království	19	17	tuto roli splňuje GOVCERT (založený roku 2007)	vládní subjekty	vedle toho v zemi existuje dalších 18 subjektů, plnících funkci CERT pro určité klienty (MODCERT pro armádu, další pro konkrétní operátory, univerzity, zákazníky soukromých firem či výzkumných ústavů)		ano (začátek roku 2007)
Španělsko	4	4	ano (IRIS, od roku 1995)	původně akademické subjekty, časem převážili správci domén (kteří nezářka vyšli z akademického prostředí)	v zemi existují i omezenější platformy (UPC – od roku 1994, universita Barcelona; CCN – od roku 2006 – obecní úřady; INTECTO – od roku 2007, soukromé firmy)	o produktech firmy a incidentech, které s nimi souvisí, je informováno jen velmi sporadicky, spíše v oblasti všeobecných rad; za zmínku stojí i skutečnost, že mezi lety 2002 - 2005 Ministerstvo pro veřejné záležitosti začalo plošně užívat LINUX (namísto dosavadní platformy SOLARIS) ⁶²	připravuje se

⁵⁹ Bezpečnostní rada již roku 2006 schválila rezoluci k podpoře ochrany kritické infrastruktury (obsahující výslovné zmínky o nutnosti zvýšení obecného povědomí o informační bezpečnosti a vytvoření platformy typu CERT).

⁶⁰ <http://www.alertnet.org/thenews/newsdesk/I25810282.htm>

⁶¹ <http://www.cert.si/>

⁶² <http://www.advogato.org/article/524.html>
<http://ec.europa.eu/idabc/servlets/doc?id=22054>

Švédsko	3	3	tuto roli nejlépe splňuje SITIC (založený roku 2003)	vládní a nevládní sektor (realizační tým stojí na základech akademického sektoru, stejně jako zde působí konkrétní soukromé subjekty: operátoři, poskytovatelé, asociace výrobců) ⁶³	v zemi existuje ještě akademická platforma SUNET (od roku 2000) a TSCERT (telekomunikační firma Telia, od roku 1997)	nepodařilo se zjistit	ne
Švýcarsko	5	4	ne	-	v zemi existuje pět platforem, omezených na konkrétní klientelu (zákazníci telefonních firem a operátorů, jaderný výzkum atd.)	nelze v konečném důsledku zjistit, konkrétní platformy nejsou neautorizovaným subjektům přístupné	ne
Turecko	2	0	ne	-	v zemi existuje platforma TR-CERT (od roku 2003), sloužící vládním a vojenským strukturám ⁶⁴ a akademická struktura ULAK (od roku 2007)		ne
Ruská federace	2	1	ano (RU-CERT, od roku 1998)	dominantní polostátní telekomunikační společnost	vedle toho existuje omezenější soukromá platforma WEBPLUS (od roku 2000)	obecně jsou vztahy Ruské federace a firmy Microsoft proměnlivé a do značné míry zpolitizované; otevřeně prezentované snahy o plošné zavedení platformy LINUX ve státní správě Ruské federace (o kterém se hovořilo roku okolo 2003), bylo nahrazeno mnohem vstřícnějšími vztahy s firmou Microsoft; RU-CERT jako polostátní subjekt s těmito posuny koresponduje, nyní je Microsoft uváděn jako jeden z jeho sponzorů	ne

⁶³ <http://www.sitic.se/> (prezentace CERT-SE)

⁶⁴ Klíčovou roli při zajišťování kybernetické bezpečnosti Turecka sehrávají ozbrojené síly (včetně aspektu financováním laboratoří k testování a auditu informačních technologií). TR-CERT dnes slouží takřka výlučně k monitorování incidentů v rámci vojenské infrastruktury (a jeho provoz je rovněž financován z armádního rozpočtu).