BUDOVÁNÍ VLÁDNÍHO PRACOVIŠTĚ CERT V ČESKÉ REPUBLICE
INFORMACE

Obsah

Úvod

Nedílnou součástí preventivní a aktivní ochrany počítačů a počítačových sítí je trvalá, důsledná a efektivní eliminace bezpečnostních incidentů, tj. jejich předcházení, řešení a odstraňování jejich 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 obnovení procesů při minimalizaci škod. Problematika zvládání incidentů tohoto charakteru je v řadě zemí světa řešena tzv. CERT týmy (Cyber Emergency Response Team).[1]

Vrcholový (národní, vládní) CERT v každé zemi představuje mimo jiné funkce také poslední záchytný bod pro řešení konkrétního problému počítačových sítí, který uživatel (firma, občan, veřejná instituce) nezvládá řešit vlastními silami nebo s pomocí příslušných správců sítě. Je samozřejmě vhodnější, když mezi uživateli a vrcholovým CERT týmem existuje ještě alespoň jeden CERT nižší úrovně, který řeší pouze problémy počítačové sítě určité firmy, veřejné instituce apod. nebo problémy počítačů, které poskytují nějakou službu (připojení k internetu, provoz specializovaného serveru apod.). V případě kybernetického útoku ze zahraničí je komunikace mezi vrcholovými CERT týmy v jednotlivých zemích světa velmi rychlá a efektivní.

V České republice však jednoznačně určený vrcholový CERT tým zatím neexistuje, ačkoli se na toto téma vedou diskuse již přinejmenším od roku 2000, a navzdory tomu, že termín prvního úkolu vytvořit takové pracoviště byl stanoven již na 30. červen 2002. Česká republika je – vedle Kypru – jedinou členskou zemí Evropské unie, kde takováto platforma zřízena nebyla.[2] Pokračování tohoto stavu je naprosto neudržitelné a vyžaduje bezodkladnou akci.

Tato skutečnost je – a to přinejmenším několik posledních let – předmětem řady nevybíravých komentářů v rámci specializovaných magazínů a internetových stránek. Veřejná správa, respektive přímo Ministerstvo vnitra, z těchto komentářů vychází značně nelichotivě.[3]

[1] Často užívaným synonymem tohoto pojmu je CSIRT (Cybernetic Security Incident Response Team).
[2] *National Computer Security Incident Response Teams* <http://www.cert.org/csirts/national/contact.html>.
[3] Například viz: Peterka, J., CSIRT, nebo CERT?; in: DSL.cz, 8. IV. 2008 <http://www.dsl.cz/clanek/1028-CSIRT,-nebo-CERT>.

Historie budování pracovišť typu CERT v České republice

Téma vybudování vrcholové hierarchie pracovišť typu CERT v České republice přitom patří mezi „chronické“ součásti seznamu nesplněných úkolů v oblasti informační bezpečnosti České republiky přinejmenším během posledních deseti let.

Úkol tohoto druhu 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).

Někdejší Ministerstvo informatiky zařadilo do dokumentu „Akční plán plnění opatření Národní strategie informační bezpečnosti České republiky“ obdobné úkoly (původně pro Ministerstvo informatiky, jejichž plnění však později přešlo na Ministerstvo vnitra): „Realizace systému včasného varování a reakce. Ustavit národní centrum pro řízení, monitoring a analýzu bezpečnostního prostředí informačních a komunikačních systémů České republiky. Ustanovení „pracoviště“ typu CERT s národní gescí.“ (gesce: Ministerstvo vnitra ve spolupráci s Bezpečnostní informační službou; termín: 2008). „Realizace aktivní mezinárodní spolupráce. Zapojit se do vytváření národních a mezinárodních pozorovacích a varovných sítí, které dokáží odhalit a zabránit elektronickým útokům v době vzniku. Zajištění uvedených činností prostřednictvím ustanovení „pracoviště“ typu CERT s národní gescí.“ (gesce: Ministerstvo vnitra ve spolupráci s Bezpečnostní informační službou a Ministerstvem obrany; termín: 2008).

Je objektivní skutečností, že funkční CERT tým výrazně zvyšuje bezpečnost jakékoliv rozsáhlé a aktivní počítačové sítě. Z toho důvodu se správci některých velkých, zvláště akademických sítí, nechovali podobně „pasivně“ jako veřejná správa ale začali efektivně vytvářet pracoviště vlastní.

Historický prvním pracovištěm typu CERT v České republice byl tým CESNET-CERTS[4], tedy první domácí subjekt typu CSIRT/CERT, disponující příslušnými praktickými zkušenostmi a napojený na relevantní nadnárodní platformy. CESNET-CERTS byl ustaven v lednu 2004, je provozován sdružením CESNET[5] a jeho hlavním úkolem je řešení a koordinace řešení bezpečnostních incidentů v páteřní akademické počítačové síti České republiky. CESNET2, jak se nazývá současná generace této sítě, je národní vysokorychlostní počítačová síť určená pro vědu, výzkum, vývoj a vzdělávání. Propojuje největší univerzitní města České republiky okruhy s vysokými přenosovými rychlostmi. Uživateli sítě jsou především vysoké školy, Akademie věd České republiky, ale i některé střední školy, nemocnice či knihovny.

[4] CESNET-CERTS, „O nás“ <https://csirt.cesnet.cz/>.
[5] CESNET: Síť pro výzkum, výzkum pro síť <http://www.cesnet.cz/>.

Deklarované cíle týmu CESNET-CERTS jsou následující:

- Zajišťovat jednoduchý a důvěryhodný kontakt pro celou síť CESNET2.
- Koordinovat řešení a prevenci bezpečnostních incidentů v síti CESNET2.
- Pomáhat institucím připojeným k síti CESNET2 vytvořit jejich bezpečnostní strategie týkající se provozu sítí a služeb.

V prostředí sítě CESNET2 působí ještě následující bezpečnostní týmy, které de facto plní roli CERT/CSIRT týmů:

- CSIRT tým počítačové sítě VŠB-TU Ostrava[6] (založen v r. 2008 a zaměřen na řešení bezpečnostních incidentů počítačové sítě VŠB-TU Ostrava),
- WIRT – WEBnet Incident Response Team Západočeské univerzity[7] (založen také v průběhu roku 2008 a zaměřen na prošetřování a řešení stížností či hlášených bezpečnostních incidentů Západočeské univerzity v Plzni),
- VUT Computer Security Incident Response Team Vysokého učení technického,
  v Brně[8] (zodpovědný za řešení incidentů v rámci počítačové sítě Vysokého učení technického v Brně),
- CSIRT-MU Masarykovy university v Brně, který však vyvíjí ještě další aktivity mimo síť CESNET2 a je navíc individuálně mezinárodně akreditován. Proto je níže uveden rovněž samostatně.

Od září 2008 funguje bezpečnostní tým regulátora odpovědného za doménu CZ, sdružení CZ.NIC (CZ.NIC-CSIRT)[9]. Platforma CZ.NIC, zájmové sdružení právnických osob, byla založena roku 1998 předními poskytovateli internetových služeb (dnes se jedná o cca 75 členů). Podle informací, které sdružení o sobě zveřejňuje, je hlavní činností sdružení provozování registru doménových jmen CZ, zabezpečení provozu domény nejvyšší úrovně CZ a osvěta v oblasti doménových jmen. Od roku 2003 funguje doména CZ v tzv. decentralizované správě, což znamená, že samotný CZ.NIC se pouze stará o funkčnost systému domény CZ, avšak prodej domén druhého řádu koncovým uživatelům provádějí jiné komerční subjekty (akreditovaní registrátoři), s nimiž má sdružení uzavřenu smlouvu. Prostřednictvím nich se také provádí veškeré změny a administrativní záležitosti.

Tým CZ.NIC-CSIRT je zodpovědný zejména za řešení incidentů dotýkajících se nameserverů (tedy hierarchicky uspořádaných serverů, na kterých jsou realizovány vzájemné převody doménových jmen a kódovaných (IP) adres uzlů sítě) pro doménu CZ. Sdružení CZ.NIC je oprávněno dle svého uvážení zrušit delegaci Doménového jména, jestliže je Doménové jméno užíváno takovým způsobem, že dochází k ohrožení národní či mezinárodní počítačové bezpečnosti, a to zejména tím, že prostřednictvím Doménového jména, či služeb, které jsou jeho prostřednictvím dostupné, dochází k distribuci škodlivého obsahu (zejm. viry, malware), nebo je předstírán obsah jiné služby (zejm. phishing), nebo hardware dostupný

[6] CSIRT tým počítačové sítě VŠB-TU Ostrava https://idoc.vsb.cz/cit/tuonet/info/csirt/index.html>.
[7] Západočeská universita: Wirt – Webnet Incident Response Team <http://support.zcu.cz/index.php/wirt_-_webnet_incident_response_team>.
[8] Vysoké učení technické v Brně: VUT Computer Security Incident Response Team (CSIRT) <http://www.vutbr.cz/portal3/index.php?page=document&wapp=webcis&parent=2&tail=2&dcid=13471&p4rew=done>.
[9] Tým CZ.NIC-CSIRT <http://www.nic.cz/csirt/>.

prostřednictvím Doménového jména je řídícím centrem sítě propojeného hardware distribuujícího škodlivý obsah (zejm. botnet).

Nejnověji v květnu 2009 vznikl na Ústavu výpočetní techniky Masarykovy university v Brně tým CSIRT-MU[10] a jeho primárním účelem je řešení bezpečnostních incidentů ve své vysokoškolské počítačové síti. Jako své hlavní cíle uvádí:

- Vytvoření jednotného důvěryhodného styčného bodu pro hlášení bezpečnostních incidentů v univerzitní síti Masarykovy Univerzity.
- Koordinování řešení bezpečnostních incidentů, především pocházejících z vnitřní sítě, a prevence takových incidentů.
- Pomoc lokálním správcům výpočetní techniky na fakultách a ústavech MU zajistit lepší bezpečnost počítačů a sítě pod jejich správou.

V přehledu budování pracovišť typu CSIRT/CERT v České republice je třeba zmínit i dvě realizované aktivity, na nichž se podílejí orgány veřejné správy, konkrétně Ministerstvo vnitra a Ministerstvo obrany.

Pro naplnění stanovených úkolů v předcházejícím textu zmiňovaného dokumentu Akční plán plnění opatření Národní strategie informační bezpečnosti České republiky bylo uspořádáno výběrové řízení na projekt Bezpečnostního výzkumu Ministerstva vnitra pro roky 2007 – 2010 „Problematika kybernetických hrozeb z hlediska bezpečnostních zájmů České republiky“ kde zvítězilo konsorcium zástupců několika fakult University Karlovy, Českého vysokého učení technického, sdružení CESNET a společnosti NESS Czech. Jedním z úkolů projektu bylo vybudování „koordinačního modelového pracoviště typu CSIRT“ (CSIRT.CZ).[11] Pracoviště se začalo vytvářet v prostorách CESNET v polovině roku 2007 a začátkem dubna 2008 byl spuštěn jeho pilotní provoz. Pracoviště pořádalo kladně hodnocená metodická zaměstnání (za účasti řady soukromých subjektů i 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 pravděpodobně zabránila nejistota o jeho budoucnosti po roce 2010.

Projekt obranného výzkumu Ministerstva obrany na roky 2008 – 2012 CYBER – Bezpečnost informačních a komunikačních systémů AČR – on line monitorování, vizualizace a filtrace paketů, rozvoj schopností Computer Incident Response Capability v prostředí Cyber Defence (CYBER)[12] řeší Ústav výpočetní techniky a Fakulta informatiky Masarykovy univerzity v Brně. Cílem projektu je analýza jednotlivých druhů hrozeb (vzorů chování) a specifikace postupů a metodik, jak naplnění těchto hrozeb odhalit a bránit se jim, formulace báze znalostí umožňující reagovat na bezpečnostní hrozby automaticky a ověření možností využití pokročilé síťové sondy při aktivní obraně datové sítě. Důležitou součástí projektu, která poskytuje bezprostřední zpětnou vazbu k aktuálním výsledkům, je praktické nasazení sond do síťového provozu, a to jak v rámci otevřené počítačové sítě MU týmem CSIRT-MU, tak i v uzavřené počítačové síti Ministerstva obrany ČR týmem CIRC MO

[10] Masarykova universita: CSIRT-MU <http://www.muni.cz/ics/services/csirt>.
[11] CSIRT-CZ: Úvod <https://www.csirt.cz/>.
[12] Masarykova universita: Projekt CYBER <http://www.muni.cz/ics/research/cyber/>.

(Computer Incident Response Capability). Tým CIRC MO – České vojenské středisko kybernetické obrany je součástí aktivit NATO usilujících o vytvoření kapacit schopných detekovat a odvracet kyberútoky proti komunikačním a informačním systémům NATO (NATO Computer Incident Response Capability – NCIRC).[13] Práce tohoto týmu je zjevně převážně neveřejná, přesto lze nalézt informace o jeho úspěšné účasti na cvičení NATO Cyber Coalition 2010[14] či odhalení nebezpečného viru (botnetu) Chuck Noris.[15]

Pohledem „zvenku" shrnuje situaci evropská platforma TERENA[16], která uvádí, že v současnosti v České republice existují čtyři CERT týmy se statusem „listed", z nichž akreditovány („accredited" – akceptován jako tým, který naplnil podmínky pro označení za CERT tým) jsou dva (CESNET-CERTS, akreditován 27. ledna 2008 a CZ.NIC-CSIRT, akreditován 26. srpna 2010), jeden je uveden jako kandidát na akreditaci („accreditation candidate") (CSIRT-MU, kandidát na akreditaci od 4. listopadu 2010) a u jednoho (CSIRT.CZ) není uvedeno nic.

[13] NATO: NCIRC, The NCIRC Technical Centre's Mission <http://www.ncirc.nato.int/index.htm>.
Základní přehled aktivit NATO v této oblasti viz např.: Zlatohlávek, P.; NATO se vrhá na ochranu kyberprostoru. Co (z)může?; in: NATO Quarterly Review, vol 6, 4/2008 – 1/2009
<http://data.idnes.cz/soubory/na_knihovna/a090603_m02_nqr_2008_4_2009_1.pdf>.
[14] *Giannetti, G., Česko poprvé vstoupilo do kybernetické války – a uspělo; in: On War – On Peace, 19. XI. 2010*
<http://www.onwar.eu/2010/11/19/cesko-poprve-vstoupilo-do-kyberneticke-valky-%E2%80%93-a-uspelo/>.
Česká republika na cvičení NATO Cyber Coalition 2010; in: Ministerstvo obrany, 19. XI. 2010
<http://www.army.cz/informacni-servis/zpravodajstvi/ceska-republika-na-cviceni-nato-cyber-coalition-2010-49559/>.
[15] Masarykova universita: Botnet Chuck Norris <http://www.muni.cz/ics/research/cyber/chuck_norris_botnet>.
Krmíček, V.; Kaderka, J.; Čeleda, P., Projekt obranného výzkumu „CYBER": Bezpečnost informačních a komunikačních systémů Armády České republiky, Bezpečnostní konference KIS, Černá Hora, 22. IV. 2010
<http://www.muni.cz/ics/research/cyber/files/cyber-kis.pdf>,
Čeští experti odhalili vir „Chuck Norris", slídil v počítačích po celém světě; in: i-Dnes, 15. II. 2010
<http://zpravy.idnes.cz/cesti-experti-odhalili-vir-chuck-norris-slidil-v-pocitacich-po-celem-svete-1t1-/zpr_nato.asp?c=A100215_153007_zpr_nato_inc>.
[16] Trusted Introducer for CSIRTs in Europe <http://www.trusted-introducer.org/>.

Budování hierarchie pracovišť typu CERT v České republice

Plán dalších kroků v této oblasti je v základních rysech následující:

- Budou vytvořeny dva vrcholové CERT týmy.
- Národní CSIRT již je vybudován na základě pracoviště firmy CZ.NIC s využitím zkušeností a kontaktů modelového pracoviště, provozovaného v rámci výzkumného projektu Ministerstva vnitra firmou CESNET (CSIRT.CZ). Jako „Národní CSIRT“ je provozován od 1.1.2011 na základě memoranda mezi ministerstvem vnitra České republiky a nezávislým sdružením právnických osob CZ.NIC. Činnost národního CSIRTu spočívá ve funkci tzv. Last resortu a Point of contact, tedy místa, kde vlastník event. napadené sítě hlásí fakt, že není v jeho silách se s útokem vyrovnat. V oblasti sítí užívaných širokou veřejností, komerční a akademickou sférou vykonává národní CSIRT i monitorovací činnost. Dočasně (do zahájení činnosti vládního pracoviště CERT) vykonává i funkci vládního CERTu a to pro vládní sítě a sítě prvků kritické infrastruktury. Funguje ale pouze jako Last resort a Point of contact. Národní CSIRT zpracovává pravidelné reporty o zachycených a řešených incidentech a předkládá je odboru kybernetické a informační bezpečnosti ministerstva vnitra. Modelově je též testována věcně příslušná komunikace s BIS. V případě závažných incidentů, zvláště pak těch, které se týkají vládních síti a sítí prvků kritické infrastruktury, informuje neprodleně a konzultuje možná řešení. V současné době je ustanovován kontrolní orgán se zastoupením ministerstva vnitra, který po zahájení plného provozu národního CSIRTu (po převzetí všech technologií a procesů z modelového pracoviště) bude mj. směrovat činnost národního CSIRTu a vypracovávat výroční zprávy.
- Od 1. 1. 2012 bude vybudován „vládní“ CERT tým (GovCERT.CZ[17]). Toto pracoviště bude primárně určeno k monitoringu vládních sítí a sítí kritické 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:

- Analyzovat současný stav (potřeby, prostorové, technické a systémové možností) co se týče zajišťování střechových funkcí v oblasti informační bezpečnosti v České republice.
- Zahájit vývoj procesů a standardů pro komunikaci tohoto pracoviště s ostatními obdobnými pracovišti v České republice i ve světě. Zajistit monitorovací, analytické a další aktivity tohoto pracoviště, včetně schopnosti efektivního vyrozumění státních orgánů, institucí, subjektů kritické infrastruktury a dalších participujících pracovišť.
- Provádět analýzu hrozeb a jejich možného odvracení prostřednictvím sběru a distribuce relevantních informací o hrozbách z/do participujících středisek doma i v zahraničí.

[17] Vzhledem ke skutečnosti, že v České republice již existuje několik platforem, nesoucích v názvu zkratku CERT respektive CSIRT, je vhodné 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.

Celý proces budování této platformy bude zřejmě postupovat „od omezenějších“ k „ambicióznějším“ cílům. Zprvu se tak zřejmě omezí na počítačové sítě, přímo spravované ústředními orgány státní správy.
Je zatím předčasné hovořit o hierarchizaci mezi oběma vrcholovými pracovišti. Oba týmy je třeba chápat spíše jako „navzájem si odlehčující partnery“. Je však třeba zajistit, aby ve sporných případech patřilo „vládnímu“ týmu právo veta (a aby tento stav byl náležitě legislativně podchycen).
Vazby obou subjektů (zejména „vládního“ pracoviště) na „armádní“ pracoviště obdobného typu (CIRC.CZ) budou předmětem dalších jednání v rámci relevantních pracovních skupin.

Předpokládané personální obsazení vládního pracoviště CERT

(může se změnit po zpracování analýz, viz níže.)

Funkce	činnost	režim	vzdělání	obor	jazyk/ stupeň	prověrka min - opt	počet ve směně	celkem
Operátor	sledování "obrazovek", prvotní analýza	24*7	Bc.	systémy ICT	A/2	D - T	3	15
Analytik	Analýzy, testování, základ pro případný Rapid team	8,5*5 + pohotvost na telefonu	Ing. Mgr.	ICT	A/2	D -T	6	6
Koordinátor	rozhoduje o řešení incidentů, řeší toky informací a operativní komunikaci s NATO,EU,BIS,PČR,UZSI apod.	8,5*5 + pohotvost na telefonu	Ing. Mgr.	Analytik s právním povědomím	A/2	D -T	4	4
PR	tvorba reportů, informačních bulletinů, call-centrum, web (veřejná i neveřejná část);	8,5*5	SŠ-Bc.		A/1	D -T	3	3
Administrátor	administrace, provoz a rozvoj systémů	8,5*5	SŠ-Bc.	ICT	A/1	D -T	3	3
Ředitel	Řízení CERTu	8,5*5	Ing.,Mgr.	ICT	A/1	T	1	1
asistent		8,5*5	SŠ-Bc.		A/1	D	1	1
						celkem	21	33

Náklady na vybudování a provoz vládního pracoviště CERT jsou prozatím odhadovány takto:

Období	1.rok		2.rok		3.rok		4.rok		5.rok	
Náklady v mil. Kč	SF	SR	SF	SR	SF	SR	SF	SR	SF	SR
Investiční náklady	80	12								
Provozní náklady	20	3	20	3	20	3	0	20	0	20
Mzdové náklady	25	3,75	25	3,75	25	3,75	0	25	0	25
Celkem	125	18,8	45	6,75	45	6,75	0	45	0	45

Poz.: SF – strukturální fondy EU, SR – státní rozpočet

Vybudování CERT a první tři roky jeho provozu budou hrazeny z prostředků strukturálních fondů EU. Ze státního rozpočtu je třeba ve prospěch Ministerstva vnitra zajistit kofinancování ve výši 15 procent celkových nákladů. V dalších letech bude nutno zajistit financování provozu z finančních prostředků státního rozpočtu České republiky.

Personální obsazení a náklady budou vyčísleny s vyšší přesností na základě analýz (viz níže), které budou vycházet z podmínek, které dosud nejsou známy.

Současný stav budování vládního pracoviště CERT

Jsou zpracovávány požadavky na provedení níže uvedených analýz, které jsou financovány z Operačního programu Lidské zdroje a zaměstnanost (64.00004). Na základě těchto analýz bude možno upřesnit všechny parametry vládního pracoviště CERT od finančních, prostorových, technologických až po personální. Samotné vybudování vládního pracoviště CERT bude také financováno ze strukturálních fondů. V tomto okamžiku je podána žádost o finanční prostředky.

1. **Analýzy přímo související s vybudováním vládního pracoviště CERT (dále jen CERT)**
    a) Analýza výstupů výzkumného úkolu P-33/VZ-2007, identifikační číslo VD20072010B13 („Kybernetické hrozby z hlediska bezpečnostních zájmů České republiky“) s ohledem na jejich využitelnost při budování vládního CERTu.
    b) Analýza prostorových, technických, systémových, personálních, procesních požadavků na vybudování a provozování CERTu pro zajištění jeho monitorovacích, analytických, forenzních, komunikačních, metodických a operačních schopností.
    c) Analýza potřebných procesů a standardů pro komunikaci centra s relevantními institucemi a s ostatními obdobnými pracovišti v České republice i ve světě.
    d) Shrnutí výsledků výše uvedených analýz do zadávací dokumentace pro výběrové řízení na vybudování CERTu.

2. **Analýzy související s legislativou**
    a) Analýza právního prostředí České republiky (s porovnáním právního prostředí zemí Evropské unie a dalších zemí světa) v souvislosti s kybernetickou a informační bezpečností.
    b) Analýza všech relevantních norem, předpisů a doporučení EU a NATO a návrh postupu při jejich zapracování do stávajícího právního řádu, resp. do nového zákona o kybernetické bezpečnosti.
    c) Analýza souvisejících podepsaných, ratifikovaných, stejně jako existujících nepodepsaných a neratifikovaných smluvních závazků (např. Dohoda o boji proti kyberkriminalitě, Memorandum of Understanding apod.) a jejich dopadu na náš existující právní řád, resp. definování potřebných změn, které tyto závazky mohou vyžadovat.
    d) Zpracování věcného záměru zákona o kybernetické bezpečnosti (se zvláštním zřetelem na respektování základních lidských práv svobod a účinnou ochranu osobních údajů) s analýzou jeho dopadu do ostatních právních předpisů a návrhem jejich případných změn.

3. **Analýzy související s prosazováním bezpečnostních standardů**
    a) Analýza v současné době používaných bezpečnostních standardů, jejich dodržování a vymahatelnosti zejména ve státní správě a subjektech zahrnutých do kritické infrastruktury.
    b) Návrh implementace standardů a návrh způsobu zajištění jejich vymahatelnosti.
    c) Stanovení minimálního souboru technických prostředků, činností a požadovaných funkcí poskytovatelů i uživatelů komunikační infrastruktury ČR pro zabezpečení včasného řešení bezpečnostních incidentů.
    d) Návrh na vytvoření systému pro kontrolu dodržování a funkčnosti bezpečnostních standardů.

4. **Analýzy související s aktivitami ČR na mezinárodní úrovni v oblasti kybernetické a informační bezpečnosti.**
    a) Analýza aktivit mezinárodních institucí v oblasti kybernetické a informační bezpečnosti.
    b) Vyhodnocení dosavadního zapojení České republiky do fungování těchto institucí a činnosti zástupců České republiky v nich.
    c) Návrh na zastoupení ČR v těchto institucích.

5. **Analýzy související s účastí na cvičeních NATO, EU a organizací vlastních cvičení**
    a) Analýza požadavků NATO na zapojení ČR do cvičení Cyber Coalition
    b) Vypracování národního scénáře účasti na cvičení Cyber Coalition jeho rozšířením do rozsahu národního cvičení
    c) Definice subjektů vhodných k zapojení do národního cvičení kybernetické ochrany propojeného na cvičení Cyber Coalition

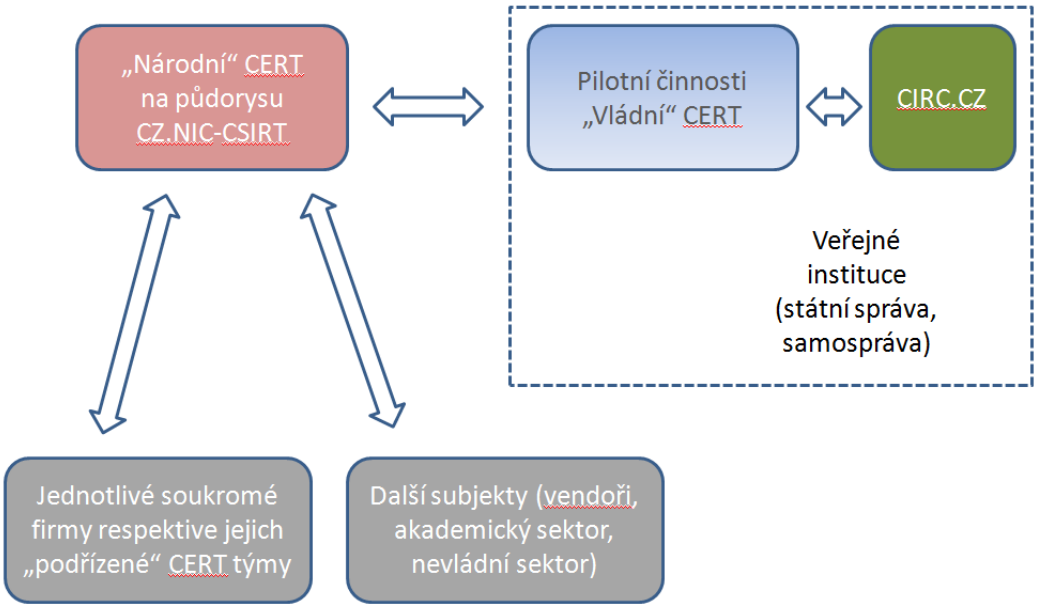
d) Definice procesů a komunikačních kanálů mezi institucemi, zapojenými do národního cvičení kybernetické ochrany propojeného na cvičení Cyber Coalition
e) Analýza požadavků na zapojení ČR do cvičení kybernetické ochrany, pořádaných EU (ENISA)

6. Analýzy související s vzděláváním a osvětou v oblasti kybernetické a informační bezpečnosti

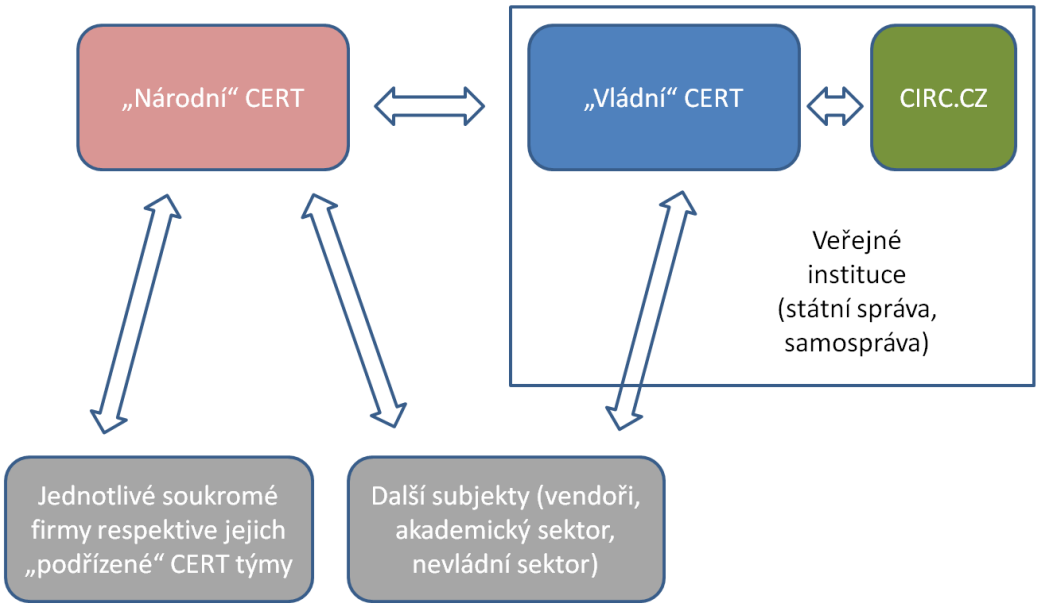
a) Analýza současného bezpečnostně právního, procesního a technicko-organizačního prostředí pro odborné vzdělávání managementu, expertů, orgánů činných v trestním řízení i koncových uživatelů informačních a komunikačních technologií.
b) Analýza možného doplnění vzdělávacích osnov všech stupňů škol o problematiku kybernetické a informační bezpečnosti.
c) Příprava public-relations kampaně k tématu rizik, souvisejících s užíváním informačních technologií se zaměřením na širokou veřejnost.

Vizualizace jednotlivých etap budování

I. fáze: (současný stav) Národní pracoviště typu CERT na půdorysu CZ.NIC-CSIRT, postupné vytváření „Vládního“ pracoviště typu CERT.



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



Týmy CERT v mezinárodním kontextu

Je třeba důrazně upozornit na skutečnost, že jedním z klíčových předpokladů funkčnosti národního CERT týmu je jeho kvalitní napojení na zahraniční protějšky, které je zpravidla formalizováno prostřednictvím „akreditace“ v klíčových nadnárodních strukturách:

- Celosvětově působící asociace FIRST (spojuje cca 200 pracovišť typu CERT).[18]
- Organizační a certifikační místo pro Evropu TF-CSIRT, spojené s organizací TERENA (v květnu 2009 sdružovalo 144 pracovišť).[19]
- Agentura Evropské unie ENISA[20], 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 trvale 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“, případně ještě "accreditation candidate").
- Akreditace.
- Certifikace (podle norem ISO[21]).

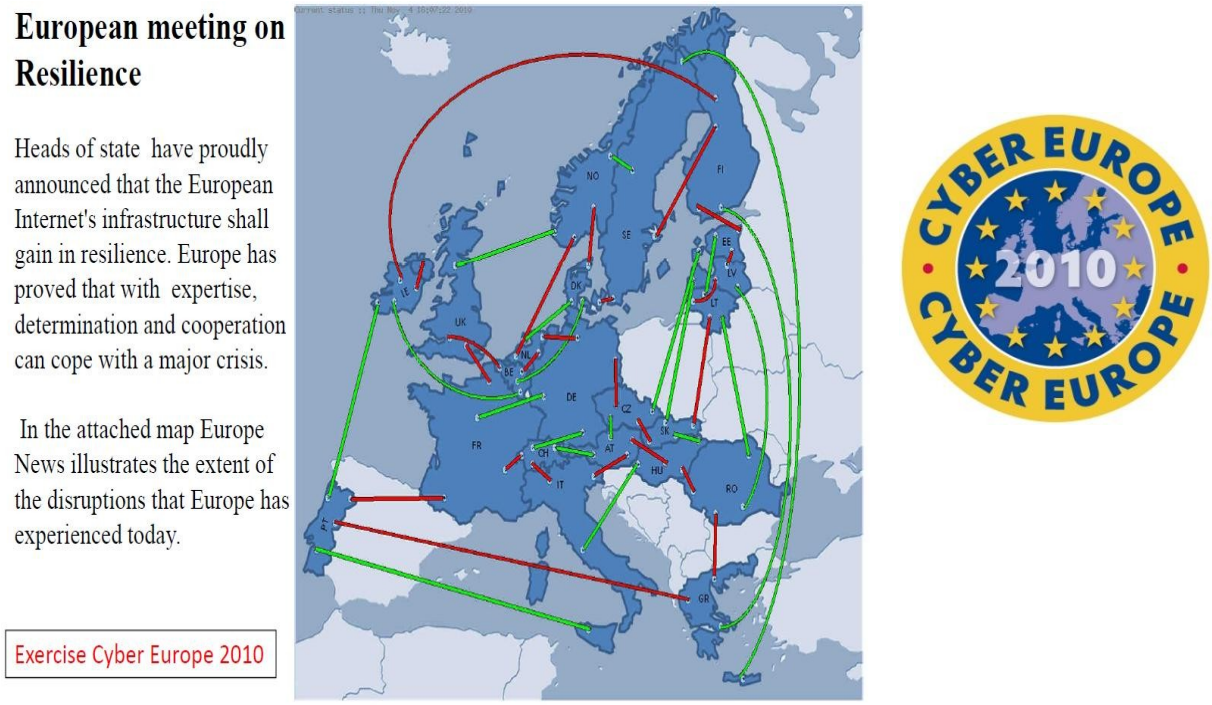
Členstvím v těchto organizacích se pak CERT pracovišti otevírá cesta k důležitým a užitečným informacím, které vytvářejí a aktualizují členské týmy, a k užší spolupráci s nimi. Organizace FIRST pořádá jednou ročně pětidenní konferenci, setkání TF-CSIRT se konají třikrát ročně. Setkání vždy hostí jeden z evropských spolupracujících týmů.

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).

[18] Forum of Incident Response and Security Teams <http://www.first.org/> (světové forum CSIRT týmů).
[19] Evropská mezinárodní organizace podporující aktivity v oblasti internetu, infrastruktur a služeb v rámci akademické komunity (*Trans-European Research and Education Networking Association*).
[20] ENISA: Security information source list, Info Sources <http://www.enisa.europa.eu/act/cert/support/guide2/annex/inf.-sources/?searchterm=index inventory>.
[21] Například systém řízení kvality (ISO 9001:2008) a informační bezpečnosti (ISO 27001:2005).

Role CSIRT/CERT pracovišť je v mezinárodním kontextu nezastupitelná. V případě kybernetického útoku, vedeného ze zahraničí, je komunikace po linii CSIRT/CERT velmi rychlá a efektivní.

Poznámka: Není bez zajímavosti, že CERT týmy roku 2010 sehrály klíčovou roli v mezinárodním cvičení CYBER Europe 2010.[22] Česká republika byla sice (po linii Ministerstva obrany) do cvičení rovněž zapojena, ale celá záležitost není ani zdaleka systémově vyřešena. Cvičení se přitom zúčastnily i státy, jejichž CERT týmy existují jen krátce (Rumunsko, Slovensko).



Ilustrace: Mapka cvičení Exercise Cyber Europe 2010 z časopisu Europe News
Evropské setkání pro odolnost.
Hlavy států hrdě oznámily, že Evropská internetová infrastruktura nabývá na odolnosti. Evropa prokázala, že odborné znalosti, odhodlání a spolupráce se dokáže vyrovnat s velkou krizí.
Přiložená mapa ilustruje rozsah narušení, které Evropa vyzkoušela.

[22] *Špecializovaný útvar CSIRT.SK sa aktívne zúčastil cvičenia CYBER EUROPE 2010, 12. XI. 2010* <http://www.csirt.gov.sk/aktuality-7d7.html?id=23>.

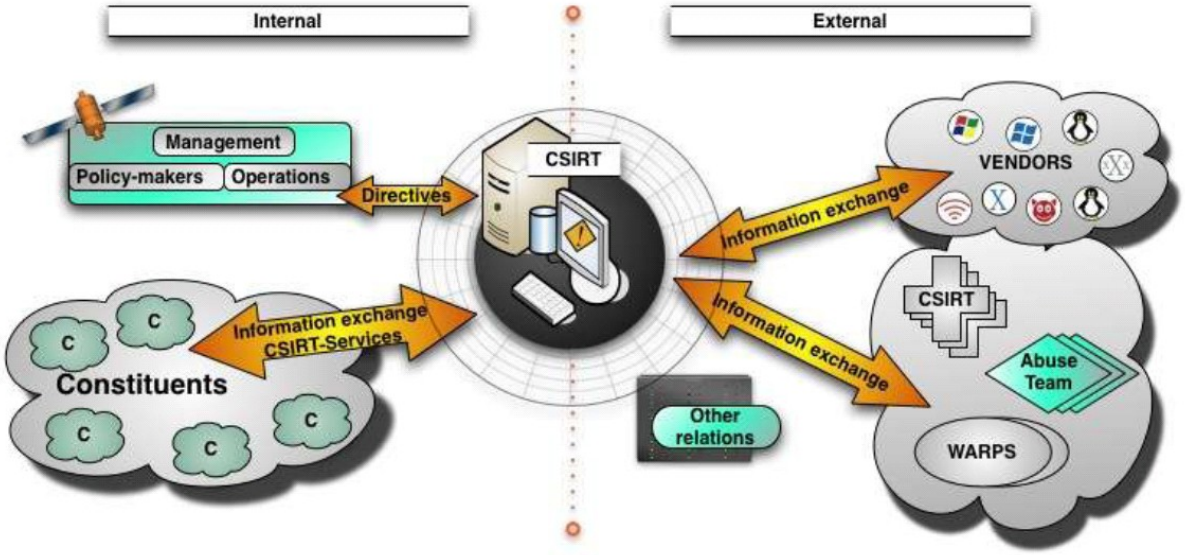
Kritéria pro určení pracoviště CERT

Konkrétní platforma se CERT pracovištěm stane v okamžiku, kdy jej ostatní již existující CERT pracoviště jako takové akceptují a naváží s ním základní spolupráci. Cesta k získání statutu CERT 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.

Služby nabízené CERT pracovištěm mohou zahrnovat služby reaktivního i proaktivního charakteru (školení, varování před aktuálními útoky, slabinami 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“) ve zkratce CERT.



Ilustrace: Pozice CSIRT/CERT pracoviště jako uzlového bodu v informační síti.[23]
Na obrázku je základní modelové schéma fungování CERT(CSIRT) v organizaci. Uprostřed je pracoviště CERT(CSIRT), které si navenek vyměňuje informace (information exchange) o kybernetických hrozbách a zranitelnostech s výrobci (Vendors) operačních systémů, aplikací, hardware apod. Dále probíhá intenzivní výměna informací mezi pracovištěm CERT a ostatními pracovišti podobného zaměření – CSIRTy podnikovými, univerzitními atd., dále s Abuse týmy (týmy , které shromažďují hlášení o hrozbách), WARPS (Warning, advice and reporting point – kontaktní bod pro varování, poradenství a reportování hrozeb - podobně zaměřená pracoviště jako CERT, ovšem s podstatně menším záběrem). Výměna informací probíhá i s dalšími institucemi s různou úrovní vazeb (other relations). Dovnitř instituce (university, firmy, ale i státu) Poskytuje CERT služby tzv. složkám (constituents), což jsou příjemci služeb a i zde probíhá výměna informací. V poslední části obrázku je naznačen vztah k managementu, který definuje politiky (policy-makers) a rozhoduje o provádění zásadních operací (operations).

[23] ENISA (European Network and Information Security Agency): Procedure for New Constituents <http://www.enisa.europa.eu/act/cert/support/guide2/external-relations/constituency/new-constituents>.

Fungování platforem typu CERT v některých zemích světa

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

- V řadě zemí existuje více či méně plnohodnotné „Národní pracoviště typu CERT“, sloužící nejširší veřejnosti (takový stav je ve 25 z celkových 27 zemí Evropské unie, dále v Ruské federaci, na Ukrajině, ve Švýcarsku, v Norsku či Chorvatsku). Vedle takového pracoviště může působit libovolný počet omezenějších platforem typu CERT, zajišťujících servis pro konkrétní zákazníky.
- V některých zemích existují pouze omezené struktury tohoto typu, které nicméně někdy
  (na požádání zahraničních partnerů) s větší nebo menší úspěšností „suplují“ roli národních CERT pracovišť (Česká republika, Island, Kypr).
- Funkční CERT slouží zejména vládním a vojenským strukturám (Turecko).
- V některých zemích tyto struktury vůbec neexistují (Bosna a Hercegovina, Makedonie, Albánie, Srbsko a Černá Hora).

Národní pracoviště typu CERT je v Evropě v současnosti nejčastěji provozováno nevládními (akademickými) subjekty (se slabší nebo silnější podporou státu). V jiných zemích provozují Národní pracoviště typu CERT pouze orgány státní správy.

Kontaktní údaje pracovišť typu CERT v České republice

CESNET-CERTS
CESNET, z. s. p. o., Zikova 4, 160 00 Praha 6
telefon: 00 420 224 352 994
e-mail: certs@cesnet.cz
http://www.csirt.cesnet.cz

CSIRT.CZ
CZ.NIC, z.s.p.o., CSIRT Team, Americká 23, 120 00 Praha 2
telefon: 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/

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/

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