Národní CSIRT České republiky

Andrea Kropáčová, andrea@csirt.cz
CSIRT.CZ
4. 8. 2011

- **CERT**
  - **C**omputer **E**mergency **R**esponse **T**eam
- **CSIRT**
  - **C**omputer **S**ecurity **I**ncident **R**esponse **T**eam

- Poskytuje služby a podporu v oblasti bezpečnosti počítačových sítí a služeb a to především v oblasti ***řešení bezpečnostních incidentů***
- Obecně bod, kam je možné obrátit se se zjištěným bezpečnostním problémem nebo i jen s podezřením.

Národní CSIRT ČR

- 16. prosince 2010 podepsáno Memorandum o CSIRT České republiky mezi MV ČR a CZ.NIC
  - http://www.nic.cz/page/830/cz.nic-ohlida-kybernetickou-bezpecnost-ceske-republiky/
- Zrozen z týmu CSIRT.CZ
- Od 1. ledna 2011 provozován CZ.NIC
- Plní také roli Vládního CSIRT ČR (dočasně)

CSIRT.CZ (2008 – 2010)

- Začal jako „modelové pracoviště typu CSIRT“
- http://www.csirt.cz/
- Dílčí úkol projektu “Kybernetické hrozby z hlediska bezpečnostních zájmů ČR”
  - Řešením byl pověřen CESNET
- Projekt „Kybernetické hrozby“:
  - zadavatel MV ČR
  - řešen v letech 2007 – 2010
  - řešen Konsorciem = VŠ, CESNET, NESS

CSIRT.CZ (2008 – 2010)

- Služby:
  - Reakce na hlášení bezpečnostního incidentu
- Role "**poslední záchrany**" pro hlášení BI v ČR
  - Pokrývá všechny adresové rozsahy přidělené do ČR
  - Kontakt - abuse@csirt.cz
  - Negarantuje úspěch, ale udělá pro něj maximum
- Pracovní skupina CSIRT.CZ
  - Zástupci ISP, bank, bezpečnostních složek, ČTU, NIX, CZ.NIC

CSIRT.CZ v datech

- Výstavba zahájena na podzim 2007
- Provoz spuštěn 3. dubna 2008
- Květen 2008 – představen světové infrastruktuře
- Červen 2008 – úřad TI potvrdil status „listed“
- Únor 2010 – vznik oddělení Kybernetické bezpečnosti MV ČR
- Prosinec 2010 – MV ČR deklarovalo vznik Národního CSIRT ČR
- Leden – červen 2011 transfer agendy od CESNET do CZ.NIC
- Červen 2011 – vstup do akreditačního procesu u úřadu TI

Role Národního CSIRT

- Důvěryhodný zdroj
  - kontaktů
  - informací a dat
- Rozvoj bezpečnostní infrastruktury:
  - pomoc se zřizováním pracovišť CSIRT
  - tvorba doporučení, návodů, pravidel...
  - vývoj nástrojů a mechanismů pro *incident handling*
- Služby:
  - reaktivní
  - proaktivní

Role Národního CSIRT

- Spolupráce mnoha sektorů:
  - Vláda, orgány státní správy, bezpečnostní složky
  - Komerční sféra - ISP, banky, finanční sektor
  - Akademická sféra, vědecká pracoviště
  - Kritické služby a infrastruktura (doprava, zásobování...)
  - Bezpečnostní týmy (CERT, CSIRT ...)
- Vazby
  - Rychlé a důvěryhodné komunikační kanály
  - Bezpečná výměna informací

Role Národního CSIRT

- Odbourává jazykové bariéry
- Zpětná vazba pro
  - tvorbu a úpravu legislativy
  - školství
- Role “poslední záchrany” (**last resort**) při řešení bezpečnostních incidentů, když:
  - není jasné, kdo je za incident zodpovědný
  - není snaha incident řešit
  - velmi závažné incidenty

Role CSIRT v národní bezpečnosti

- Kooperace vládního a soukromého sektoru
- Tvorba a údržba komunikačních kanálů
- Zabezpečená výměna a sdílení informací
- Připravené mechanismy pro:
  - koordinaci obrany
  - včasné varování
  - analýzu problému a návrh řešení
  - krizové plány a plány obnovy
- Sledování trendů v oblasti bezpečnosti

CSIRT.CZ

- Aktuální stav:
  - Dokončen transfer agendy a technologií
  - Plně ve správě CZ.NIC
  - 25. července – „accreditation candidate“
- Pracuje se na:
  - Udržení spolupráce
  - Koncepci fungování
  - Definování role a vazeb v ČR
  - Definování služeb

Česká republika

- Oficiálně konstituované týmy (http://www.trusted-introducer.org):
  - CSIRT.CZ = Národní CSIRT ČR
  - CZ.NIC – CSIRT
  - CESNET – CERTS
  - CSIRT – MU
- Vládní CSIRT ČR je ve výstavbě
  - sítě státní správy
  - sítě samosprávy
  - sítě kritické infrastruktury

Děkuji za pozornost.

Andrea Kropáčová, andrea@csirt.cz
CSIRT.CZ
4. 8. 2011