Přínosy existence a provozu týmu typu CSIRT/CERT

Andrea Kropáčová

CESNET, z. s. p. o.

ItSMF 2010

Návratnost nákladů do zlepšování systému řízení IT

CSIRT/CERT

- **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.

CSIRT/CERT

- Je **infrastruktura**, která umožňuje
  - → Rychlejší a efektivnější reakci při řešení bezpečnostních incidentů
  - → Prevenci bezpečnostních incidentů
  - → Zvyšování bezpečnosti sítě a služeb
- Edukační prvek
  - Pro provozovatele sítí
  - Pro uživatele
- **CSIRT není nástrojem ani prostředkem represe, kontroly a regulace!**

Co dělá CSIRT CSIRTem?

- Jasně definovaná ***„constituency“ :***
  - Za co zodpovídá (část kyberprostoru/Internetu)
  - Role, zodpovědnost, pravomoc
  - Kontaktní informace
  - Odezva a reakce
  - Poskytované služby - minimem je ***řešení incidentů*** (RESPONSE)
- Optimální stav = každá jednotka kyberprostoru (Internetu) je v kompetenci některého CSIRTu

Vznik CERT/CSIRT

- Zřizovatel definuje:
  - "Constituency"
    - Model/roli – interní, koordinační, vendor, *vládní, národní* ...
    - Pole působnosti – síť, region, oblast zájmu
    - Zodpovědnost a pravomoc (mandát)
  - Služby (reaktivní, proaktivní)
- Zázemí
  - Organizační
  - Technické
  - Metodické

Služby CERT/CSIRT

- Incident handling
- Alerts & Warnings
- Vulnerability Handling
- Artefact Handling
- Announcements
- Technology Watch
- Audits/Assessments
- Configure and Maintain Tools/Applications/Infrastructure
- Security Tool Development
- Intrusion Detection
- Information Dissemination
- Risk Analysis
- Business Continuity Planning
- Security Consulting
- Awareness Building
- Education/Training
- Product Evaluation

Kdy je tým CERT/CSIRT?

- Když tým uznají již existující CERT/CSIRT týmy
  - FIRST, http://www.first.org/
  - TI (Trusted Introducer), http://www.trusted-introducer.org/
  - TF-CSIRT, http://www.terena.org/
- Čím je zaručena důvěryhodnost CERT/CSIRT?:
  - Důraz kladen na komunikaci a spolupráci
  - Musí být plně transparentní
  - Musí mít konzistentní vystupování
  - Otevřenost ke komunitě CSIRTů

CERT/CSIRT v ČR

- CESNET-CERTS (CESNET)
  - Operuje nad sítí CESNET2 (AS2852)
- CSIRT.CZ (Projekt Kybernetické hrozby, MV ČR)
  - Operuje v rámci celé České republiky
  - Zárodek “vrcholového” týmu
- CZNIC-CSIRT (CZ.NIC)
  - Operuje nad sítí CZ.NIC a TLD doménou .cz
- CSIRT-MU (Masarykova univerzita, Brno)
  - Operuje nad sítí Masarykovy university

Univerzitní CSIRT

- Přínosy z vybudování zázemí týmu
  - Standardizace postupů při řešení bezp. incidentů
  - Dokumentace – síť, zařízení, služby, uživatelé
  - Procesy, pravidla, směrnice, politiky
  - Evidence – incidentů, pachatelů, zdrojů
  - Služby
  - Bezpečnostní nástroje
    - Na detekci bezpečnostních problémů
    - Audity, forenzní analýza

Z reakcí původců incidentů

- **Z prostředí univerzitního CERT/CSIRT:**
  - *“Já jsem ty filmy nenabízel, jenom stahoval!”*
  - *“Vždyť to bylo v TV, tak si to mohu sdílet jak chci!”*
  - *“Na Internetu je přece všechno free ...”*
  - *“Licenci na OS/SW? “Půjčil” jsem si ji od kamaráda.”*
  - *“Jak víte, že jsem to byl já? Já se připojuji jenom přes wifi.”*
  - *“Nikdo mi nedokáže, že jsem to byl já!”*
  - *“Můžu dělat co chci, zaručují mi to akademické svobody!”*
  - *“Ale já jsem to napsal jenom na Facebook!”*
  - *“Ale já ten mail poslal jen 1000 uživatelům.”*

Přínos univerzitního CERT/CSIRT

- Edukace uživatelů
  - Instituce (VŠ) má pravidla pro používání sítě
  - Principy fungování Internetu a jeho úskalí
  - Ochrana dat a identity
  - Legislativa
- Chrání:
  - Dobré jméno instituce
  - Chrání Internet před vlastními uživateli
  - Uživatele před jimi samotnými

==> Snižuje páchání incidentů a recidivu

CERT/CSIRT na úrovni ISP

- PoC dané sítě
  - Pro vlastní uživatele (zákazníky)
  - Pro svět
- Rychlá reakce při vzniku bezpečnostního incidentu
  - Ochrana vlastní infrastruktury
  - Ochrana zákazníka
  - Ochrana dobrého jména společnosti
- Zdroj informací pro další vývoj sítě a služeb
- Zpětná vazba pro technické pracovníky, vývojáře, marketing, management

Z reakcí při řešení BI

- **Z prostředí CERT/CSIRT na úrovni ISP:**
  - *“Ten zavirovaný počítač opravím až později”.*
  - *“Já jsem tu jediný správce a vedení nechce přijmout dalšího”.*
  - *“My na stránkách nemáme žádný phishing, teď na ně koukám”.*
  - *“To je na stránkách našeho zákazníka, s tím já nemohu nic dělat”.*
  - *“Já bych to rád opravil, ale šéf mi přikázal udělat nejdřív tu zprávu pro management”.*

Vrcholový CERT/CSIRT

- PoC dané země
  - Poslední možnost kam se obrátit se žádostí o pomoc
  - Komunikační a koordinační prvek
- Platforma pro spolupráci
- Šíření osvěty
- Zpětná vazba, zdroj know-how a informací pro
  - Provozovatele sítí, služeb a kritické infrastruktury
  - Tvůrce legislativy
  - Bezpečnostní složky

Přínosy existence CERT/CSIRT

- **Finanční:**
  - → Rychlá reakce při vzniku bezpečnostního incidentu
    - Minimalizace škod
    - Rychlá obnova funkcionality sítě a služeb
    - Ochrana uživatelů
- **Nefinanční?:**
  - → Spolupráce, zlepšení vztahů s okolními zeměmi
  - → Výměna a sdílení informací a know-how
  - → Podpora a edukace uživatelů
  - → Zpětná vazba pro management

Zdroje a poděkování

- Tato přednáška čerpá ze zkušeností těchto týmů:
  - CSIRT tým VŠB, Ostrava
  - CSIRT tým ZČU, Plzeň
  - CESNET-CERTS, http://csirt.cesnet.cz/
  - CSIRT.CZ, http://www.csirt.cz/
  - CZ.NIC-CSIRT, http://www.nic.cz/
- Děkuji za pomoc a cenné informace kolegům Radomíru Orkáčovi z VŠB v Ostravě a Aleši Padrtovi ze ZČU v Plzni

Děkuji za pozornost.

Andrea Kropáčová, CESNET.