Přínosy zřízení a provozu CSIRT týmu v organizaci

CZ.NIC z.s.p.o.

Andrea Kropáčová / *andrea.kropacova@nic.cz*
9. 6. 2011

CZ.NIC | SPRÁVCE DOMÉNY CZ

CERT/CSIRT

Computer Emergency Response Team
Computer Security Incident Response Team

- 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.
- CERT/CSIRT týmy tvoří infrastrukturu, která umožňuje:
  - rychlejší a efektivnější reakci při řešení BI
  - prevenci bezpečnostních inicidentů
  - zvyšování bezpečnosti sítě a služeb
- Edukační prvek
  - Pro provozovatele sítí
  - Pro uživatele

CERT/CSIRT týmy v ČR

- CESNET-CERTS
  - operuje nad sítí CESNET2 (AS2852)
  - provozován CESNET
- CZ.NIC-CSIRT
  - operuje nad sítí CZ.NIC a TLD doménou .cz
  - provozován sdružením CZ.NIC
- CSIRT-MU
  - vybudován v roce 2008
  - operuje nad sítí Masarykovy university v Brně
- CSIRT.CZ

CSIRT.CZ

- Národní CSIRT České republiky
  - koordinační role při řešení incidentů („last resort“)
  - vzdělávání a osvěta v oblasti bezpečnosti
  - vznik deklarován 9. prosince 2010
  - od 1. ledna 2011 provozován sdružením CZ.NIC
- Historie:
  - založen v rámci plnění grantu „Kybernetické hrozby z hlediska bezpečnostních zájmů České republiky“ (2007 – 2010)
  - provoz spuštěn 3. dubna 2008
  - v letech 2008 – 2010 provozován sdružením CESNET

Co se očekává od CSIRT

- PoC dané sítě
  - Pro vlastní uživatele (zákazníky)
  - Pro svět
- Rychlá reakce při vzniku bezpečnostního incidentu
  - Ochrana vlastní infrastruktury
  - Ochrana zákazníka/uživatele
  - Ochrana dobrého jména organizace
- Poskytování služeb
- Spolupráce s uživateli v rámci pole působnosti týmu
- Mezinárodní i národní spolupráce

Přínosy z procesu zřízení CSIRT

- Standardizace postupů pro řešení bezpečnostních incidentů
- Dokumentace:
  - síť, zařízení, služby, uživatelé
  - procesy, pravidla, směrnice, politiky, plány obnovy
- Vývoj:
  - bezpečnostních nástrojů
  - služeb
- Evidence – incidentů, zdrojů a typů incidentů
- Spolupráce se světovou infrastrukturou
- Navázání komunikace s uživateli

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!”*
  - *„Já to zaplatím! Kam mám tu pokutu (za porušení AP) poslat?“*

Přínosy zřízení a provozu CSIRT

- Rychlá reakce při vzniku bezpečnostního incidentu
  - Rychlá obnova funkcionality sítě a služeb
  - Ochrana dat, zdrojů, know-how
  - Ochrana uživatelů

  } = minimalizace škod
- Zpětná vazba pro technické pracovníky, vývojáře, marketing, management, komunitu
- Zdroj informací pro další vývoj sítě a služeb
- Výměna a sdílení informací a know-how
- Podpora a edukace uživatelů
- Spolupráce, zlepšení vztahů s okolím
- "Sociální" efekt

Přínosy zřízení a provozu CSIRT

- Univerzitní CSIRT týmy hlásí:
  - snížení recidivy, lepší možnosti ochrany uživatelů
- Tým CZ.NIC-CSIRT
  - od roku 2010 blokuje domény se závadným obsahem
  - vývoj proaktivních služeb pro uživatele
- CSIRT.CZ, Národní CSIRT ČR
  - ČR má „místo poslední záchrany“
  - Pracovní skupina CSIRT.CZ
  - zpětná vazba pro:
    - provozovatele sítí a služeb
    - bezpečnostní složky
    - tvůrce legislativy

Zdroje a poděkování

- Tato přednáška čerpá ze zkušeností těchto týmů:
  - CESNET-CERTS, http://csirt.cesnet.cz/
  - CSIRT.CZ, http://www.csirt.cz/
  - CZ.NIC-CSIRT, http://www.nic.cz/
  - CSIRT-MU, http://www.muni.cz/csirt
  - CSIRT tým VŠB, Ostrava
  - CSIRT tým ZČU, Plzeň

Děkuji za pozornost.

Andrea Kropáčová