Budování CERT/CSIRT v organizaci

Andrea Kropáčová / andrea@nic.cz

31. března 2015

CZ.NIC | SPRÁVCE DOMÉNY CZ

CZ.NIC

- CZ.NIC, z. s. p. o.
- Založeno 1998 významnými ISP
- Aktuálně 113 členů (otevřené členství)
- Neziskový, neutrální
- 80+ zaměstnanců (Praha, Brno, Plzeň)
- Hlavní role – provoz domény .cz
  - Více než 40 registrátorů
  - Více než 1mil zaregistrovaných domén (400tis chráněno DNSSEC)
- MoU s Vládou ČR, NBÚ
- Další aktivity
  - výzkum a vývoj v oblasti bezpečnosti (MojeID, DNSSEC, IPv6, Turris)
  - provoz CSIRT.CZ (Národní CSIRT ČR)
  - Akademie – školicí středisko, vydávání knih, osvěta, soutěže, kampaně ...

CSIRT.CZ

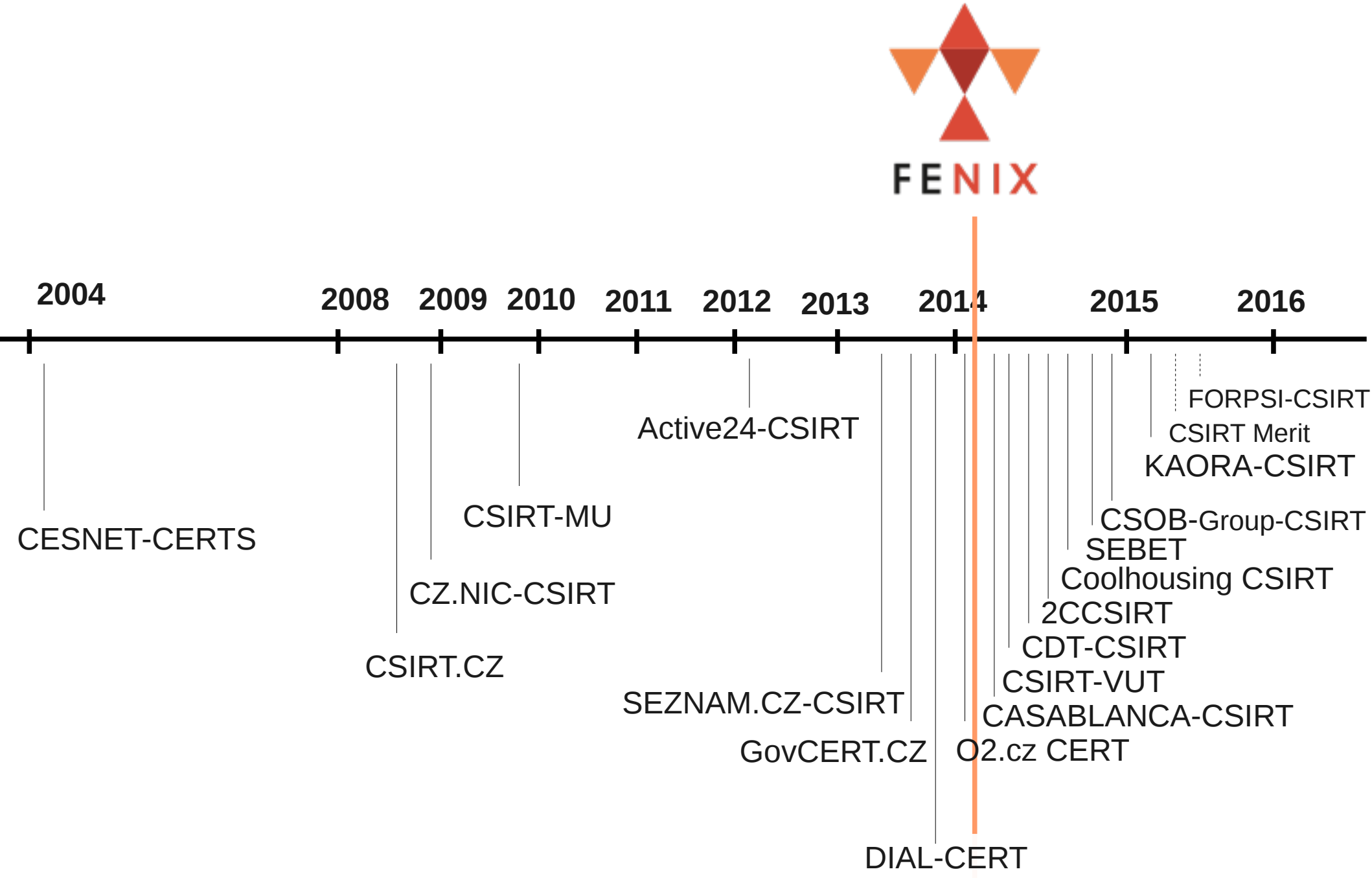
- http://www.csirt.cz/
- **Národní CSIRT České republiky**
- **Provozován sdružením CZ.NIC**
- Historie
  - Založen v roce 2008 rámci plnění grantu „Kybernetické hrozby z hlediska bezpečnostních zájmů České republiky“ (2007 – 2010)
  - V letech 2008 – 2010 provozován sdružením CESNET
  - Memorandum mezi MV ČR a CZ.NIC ze dne 9. 12. 2010
- CZ.NIC provozuje CSIRT.CZ jako Národní CSIRT ČR od 1. 1. 2011
  - Od 1. 4. 2012 provoz na základě memoranda s NBÚ
    - https://www.csirt.cz/files/csirt/Memorandum_nbu.pdf
- Status „akreditovaný“ u TI (od 2011)

CSIRT.CZ

- Členové: M. Peterka, A. Kropáčová, P. Bašta, M. Prokop, Z. Duračinská, E. Rejthar

- Kontaktní údaje:
  - *adresa sídla:* Milešovská 5, Praha 3, Česká republika
  - *www stránky:* http://www.csirt.cz
  - ***abuse@csirt.cz***
    - adresa pro hlášení kontaktních údajů
  - ***info@csirt.cz***
    - adresa pro dotazy obecného typu
  - urgentní kontakt:
    - viz TI adresář
    - non stop dohledové pracoviště CZ.NIC
      - http://www.nic.cz

Vývoj CERT/CSIRT v České republice



CERT/CSIRT in Czech Republic

(17 + 2)

2CCSIRT	Listed (since 15 Sep 2014)
ACTIVE24-CSIRT	Listed (since 09 Feb 2012)
CASABLANCA.CZ-CSIRT	Listed (since 08 Mar 2014)
CDT-CERT	Listed (since 16 Jul 2014)
CESNET-CERTS	Accredited (since 27 Jan 2008)
Coolhousing CSIRT	Listed (since 17 Sep 2014)
CSIRT-MU	Accredited (since 01 Feb 2011)
CSIRT-VUT	Listed (since 20 May 2014)
CSIRT.CZ	Accredited (since 13 Oct 2011)
CSOB-Group-CSIRT	Listed (since 29 Oct 2014)
CZ.NIC-CSIRT	Accredited (since 26 Aug 2010)
DIAL-CERT	Listed (since 16 Dec 2013)
GOVCERT.CZ	Accredited (since 21 Aug 2014)
O2.cz CERT	Listed (since 01 Jan 2014)
SEBET (ITSELF.CZ-CSIRT)	Listed (since 25 Oct 2014)
SEZNAM.CZ-CSIRT	Listed (since 18 Oct 2013)
KAORA-CSIRT	Listed (since 04 Mar 2015)
CSIRT Merit	In the process ...
FORPSI-CSIRT	In the process ...

Co znamená být CERT/CSIRT?

- Jasně definovaná ***„constituency“***:
  - Kontaktní informace
  - Členové týmu
  - Provozovatel
  - Za co zodpovídá (část kyberprostoru/Internetu):
    - AS, IP bloky, domény
    - Země, organizace, část infrastruktury
  - Role, zodpovědnost, pravomoc
  - Odezva a reakce
  - Služby
    - minimem je ***řešení incidentů*** (RESPONSE x CSIRT)
- Být součástí světové infrastruktury CERT/CSIRT týmů
- Optimální stav = každá jednotka kyberprostoru (Internetu) a každý uživatel je v kompetenci některého CSIRTu

Budování CERT/CSIRT týmu – jak začít?

- Identifikace potřeb
- Identifikace cílů
- Výběr členů a sestavení týmu
- Definování role a působnosti týmu
  - „směrem dovnitř“ = v organizaci
  - “směrem ven” = pro mezinárodní infrastrukturu
- Služby
  - minimem je ***řešení incidentů*** (RESPONSE)
  - reaktivní, proaktivní, osvětové
- Zázemí týmu
  - Organizační, technické, adiministrativní
- Určení zodpovědnosti a pravomocí
- Navázání národní a mezinárodní spolupráce

Budování CERT/CSIRT týmu – jak začít?

- Identifikace potřeb
- Identifikace cílů
- Výběr členů a sestavení tým
- Definování role a působn
  - „směrem dovnitř“ = v
  - “směrem ven” = pro
- Služby
  - minimem je ***řešení incid***
  - reaktivní, proaktivní, osvětov
- Zázemí týmu
  - Organizační, technické, adiministrativní
- Určení zodpovědnosti a pravomocí
- Navázání národní a mezinárodní spolupráce

Podpora managementu, prohlášení managementu o podpoře týmu, definování jeho role, pravomocí, zodpovědnosti.

Identifikace potřeb – proč CSIRT tým?

- Potřeba řešit incidenty (Incident Handling) ve své síti/organizaci
  - Incidenty se nevyhýbají nikomu
  - Větší organizace řeší několik denně
  - Specializované oddělení pro řešení incidentů
    - Rutinní opakovaná činnost
      - Typické druhy incidentů a jejich řešení
      - Nové varianty vždy vyžadují adaptaci
    - Má patřičné znalosti a zkušenosti (= je připraven)
    - Umí posoudit všechny dopady
    - Dokáže zkoordinovat činnost a spolupráci

Identifikace potřeb – proč CSIRT tým?

- Koordinace činností
  - Větší rozsah incidentu občas vyžaduje spolupráci
    - Uvnitř organizace
    - Spolupráce s ostatními organizacemi
  - Vyžadování znalostí
    - Technické
    - Organizační
  - Nutnost mít připravený (vycvičený) tým
    - V případě výskytu problému je už pozdě
    - Není možné zjišťovat základní věci, až když problém nastane
  - Když už CSIRT umí řešit malé rutinní incidenty, může koordinovat i závažnější
    - Kdo jiný by tomu rozuměl lépe?
    - Kdo jiný by měl potřebné zázemí a znalosti?

Identifikace potřeb – proč CSIRT tým?

- Eskalace
  - Různá závažnost vzniklých incidentů
  - Někdo musí vyhodnotit
    - Spadá ještě pod rozhodnutí bezpečnostního týmu?
    - Vyžaduje se rozhodnutí ředitele IT, manažera bezpečnosti?
    - Vyžaduje spolupráci s právníky?
    - Vyžaduje spolupráci s PČR?
    - Vyžaduje se rozhodnutí generálního ředitele?
  - Zajištění komunikace a sběr všech informací
  - Když už to CSIRT koordinuje ...
    - Část může vyřešit v rámci svěřených pravomocí

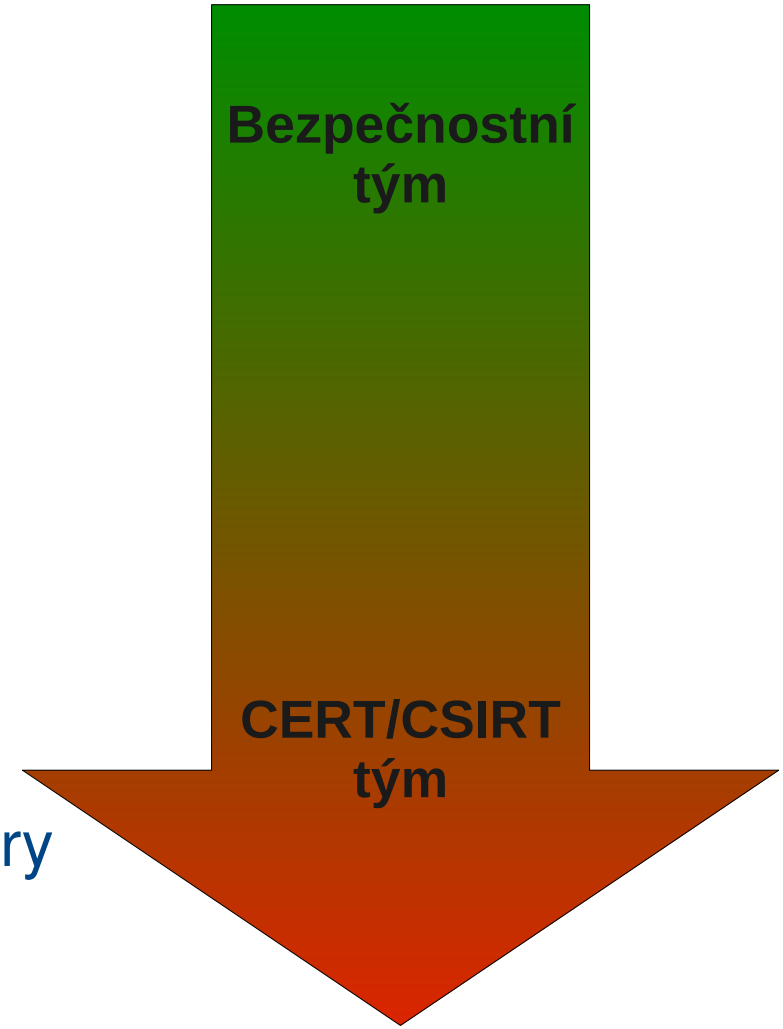
Identifikace potřeb – proč CSIRT tým?

- Standardizace
  - Časté opakování + snaha o transparentnost

    → standardizace činností:
    - Navyklá rutina
    - Pracovní postupy
    - Procesy
  - Standardizace je nevyhnutelná
  - Proč vymýšlet již vynalezené?
    - Komunita CSIRT – má zkušenosti
      - školení TERENA, ENISA, SANS
      - školení od CSIRT.CZ, GovCERT.CZ
      - návody, standardy, doporučení
      - pracovní skupiny

Identifikace cílů

- Koordinace činností
- Standardizace
- Formalizace procesů
- Eskalace procedur
- Vnitřní bezpečnost organizace
- Bezpečnostní strategie
- Poskytování a rozvoj služeb
- Renomé, pozice na trhu
- Zapojení do (mezi)národní infrastruktury
- Účast v (mezi)národních projektech



Výběr členů týmu

- Doporučuji alespoň 2, lépe 3 členy
  - ne nutně full-time
  - zástupnost
  - týmová spolupráce, diskuse
- Kvalifikace, zkušenosti, zaměření
  - měli by se odborně doplňovat
  - odborně by měli pokrýt roli týmu, cíle, služby
    - správce sítě a IT služeb
    - právník
    - specialista: penetrační testy, forenzní analýza
  - správce IT služeb je dobrý základ
    - znalost fungování Internetu a klíčových služeb
    - principy bezpečnosti
    - ochrana uživatel
- Členy CSIRT týmu je potřeba kontinuálně vzdělávat

Definování role a působnosti týmu

- V organizaci
  - nemusí být žádná
  - vnitřní bezpečnost
    - bezpečnost sítě a služeb
    - uživatelé
    - informace

} **formulování/podíl na formulování bezpečnostní strategie organizace**

- „Směrem ven“ = pole působnosti
  - obvykle technická definice
    - AS
    - doména
    - IP rozsah
  - umožňuje CERT/CSIRT infrastruktuře nalézt ten správný tým
  - co tým garantuje za akce v poli působnosti (typ interní, typ koordinační ...)

Zázemí týmu

- Organizační
  - dokument definující existenci, roli, pravomoci a zodpovědnost týmu
  - politiky provozu
    - incident handling (řešení BU a BI)
    - zacházení s citlivými informacemi
  - politiky zajištění jednotlivých služeb
  - web s popisem týmu
  - postupy, návody, know-how, work-flow ... aneb „připravenost na problém“

- Technické
  - správa hlášení bezpečnostních incidentů
  - správa požadavků
  - nástroje pro detekci BU a BI

Služby

- Měly by vycházet z potřeb organizace a cílů pro zakládání CSIRT
- Základní:
  - Incident response a incident handling
    - reagování na bezpečnostní incidenty a události
    - minimum každého CSIRT týmu
- Rozšířené:
  - varování před problémy
  - správa zranitelností, testování zranitelností
  - sběr důkazů
  - doporučení, informování
  - školení, konzultace
  - audity
  - detekce průniků

Služby

- 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

Určení role, zodpovědnosti a pravomocí

- Role
  1) tým pro řešení vnitřních otázek bezpečnosti organizace
  2) tým zajišťující 1) a zároveň je součástí světové infrastruktury
- Zodpovědnost
  - tým zodpovídá za bezpečnost sítě, služeb, uživatelů
  - tým zodpovídá za řešení bezp. událostí a bezp. incidentů
- Pravomoc
  - „může odpojit zdroj problému“
  - „může dát pokyn k odpojení zdroje problému síťovému oddělení“
  - „je oprávněn zabavit problematické PC k další analýze“
- Ukotvení v organizační struktuře
  - tým je zařazen do úseku A, podřízen přímo provoznímu řediteli úseku A
  - tým je mimo organizační strukturu a je podřízen přímo řediteli společnosti

Určení role, zodpovědnosti a pravomocí

- Role
  1) tým pro řešení vnitřních otázek bezpečnosti organizace
  2) tým zajišťující 1) a zároveň je součástí světové infrastruktury
- Zodpovědnost
  - tým zodpovídá za bezpečnost sítě, služeb, uživatelů
  - tým zodpovídá za řešení bezp. událostí a bezp. incidentů
- Pravomoc
  - „může odpojit zdroj problému“
  - „může dát pokyn k odpojení zdroje problému síťovému oddělení“
  - „je oprávněn zabavit problematické PC k další analýze“
- Ukotvení v organizační struktuře
  - tým je zařazen do úseku A, podřízen přímo provoznímu řediteli úseku A
  - tým je mimo organizační strukturu a je podřízen přímo řediteli společnosti

Národní a mezinárodní spolupráce

- FIRST, http://www.first.org/
- ENISA, http://www.enisa.eu
- CERT/CC, http://www.cert.org
- TERENA
  - TF-CSIRT
  - Trusted Introducer
    - přijímá nové týmy do infrastruktury
- CSIRT.CZ, Národní CSIRT České republiky
  - Pracovní skupina CSIRT.CZ
  - Pracovní skupina pro oficiální CERT/CSIRT týmy
- GovCERT.CZ, Vládní CERT České republiky
- Fenix, AFCEA, ISACA ...

Přínos konstituování CSIRT týmu (souhrn)

- Možnost formalizace procesů, zavedení work-flow, pravidel ...
- Skvělá příležitost k
  - revizi IT :-)
  - nastavení komunikace mezi „techniky“ a „managementem“
- Reakce na ZKB
- Možnost zapojit se do národní a mezinárodní bezpečnostní infrastruktury
  - mít se kam obrátit o pomoc nebo konzultaci
  - možnost zapojit se do mezinárodních projektů
  - sdílení informací a dat

⇒ budování důvěry, vztahů

⇒ být součástí komunity

Děkuji za pozornost

CSIRT.CZ

Andrea Kropáčová / andrea@csirt.cz