Bezpečnostní týmy typu CSIRT/CERT obecně a v CZ.NIC

CZ.NIC z.s.p.o.
Martin Peterka / martin.peterka@nic.cz
Konference Bezpečnost kyberprostoru
25. 10. 2011

CZ.NIC | SPRÁVCE DOMÉNY CZ

Obsah

- CERT/CSIRT týmy obecně
  - Co to je CSIRT/CERT
  - Typy týmů, jejich role
  - Mezinárodní ukotvení
- CSIRT v CZ.NIC
  - CZ.NIC-CSIRT
  - CSIRT.CZ

CSIRT/CERT

Computer Emergency Response Team
Computer Security Incident Response Team

- CSIRT/CERT
  - Formalizovaný bezpečnostní tým
  - Podpora v oblasti bezpečnosti, řešení bezpečnostních incidentů
  - Veřejně deklaruje :
    - svou roli,
    - pole působnosti,
    - typy služeb,
    - členy týmu,
    - zodpovědnosti a pravomoci
  - Různé modely týmů

Typy CSIRT týmů

- Typy týmů se rozlišují podle zaměření
  - Interní
  - Vendor
  - Národní
  - Vládní
  - …
- I v rámci tohoto rozlišení rozdíly

Interní CSIRT tým

- Základní stavební kámen
- Je zodpovědný za interní síť/systém/infrastrukturu konkrétní organizace
  - ISP
  - Univerzita
  - Banka
  - …
- Řeší konkrétní incidenty
  - Odstranění hrozby, nalezení napadeného počítače, smazání neadekvátního obsahu, …
- Příkladem může být CZ.NIC-CSIRT

CSIRT tým typu „vendor“

- Obvykle tým velké organizace, nabízející technologie
- Je zaměřený na vlastní technologii
  - Připravuje opravy SW/HW
  - Upozorňuje na možná nebezpečí
  - Informuje o vydání záplat
  - Spolupracuje při řešení konkrétních problémů
- Mají expertní a proaktivní úlohu
- Prodejci HW (routery, počítače, …), SW firmy (operační systémy, …), společnosti zaměřené na viry apod.
- Příklady – CISCO, Microsoft, …

Národní CSIRT

- Role národních CSIRT týmů se liší stát od státu
- Slouží jako tým typu „last resort“ pro komerční a akademickou sféru
- Plní dvě základní role :
  - Koordinační
  - Vzdělávací/osvětová
- Není zpravidla řízen/zřízen zákonem ale vznikne „odspoda“
- Nemá obvykle výkonné pravomoci
  - Neumí nic „vypnout“
- Není statistické centrum
  - Zdaleka ne všechny incidenty jsou řešeny jeho prostřednictvím, nebývá ani informován, pokud to není nutné
- Příklady – CSIRT.CZ

Vládní CSIRT

- Plní podobné role jako národní CSIRT, ale v rámci státní správy a samosprávy
- Často zřízen ze zákona
- Má výkonné pravomoci směrem ke státní správě
- Různorodé varianty
  - Od jednoduchého koordinačního centra (se silnými interními týmy jednotlivých částí státní správy)
  - Až po silné centrum s výraznými pravomocemi, včetně vyhodnocovacích (statistických) systémů a s centrálním dohledem
- V ČR v tuto chvíli zákon neexistuje

Další typy týmů

- Samozřejmě systém je složitější
- Armáda a související
- Výzkumníci (ne nutně musí být vendor)
- Forenzní týmy
- …

Komunikace při řešení incidentu

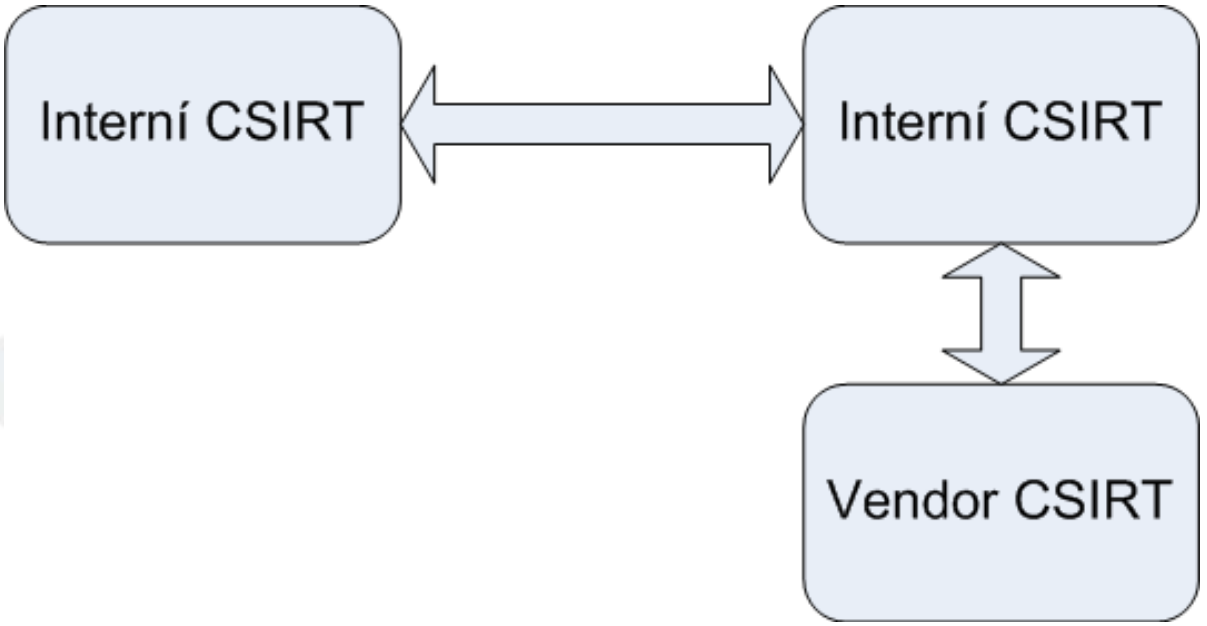
- Existuje hierarchie mezi týmy?
- Jak se navzájem najdou?
- Je nějaká centrála?
- Jiná spolupráce?

- Báze důvěry
- Často neformální spolupráce (ne mezi institucemi, ale lidmi)
- Mezinárodní organizace

Typy komunikace – I.

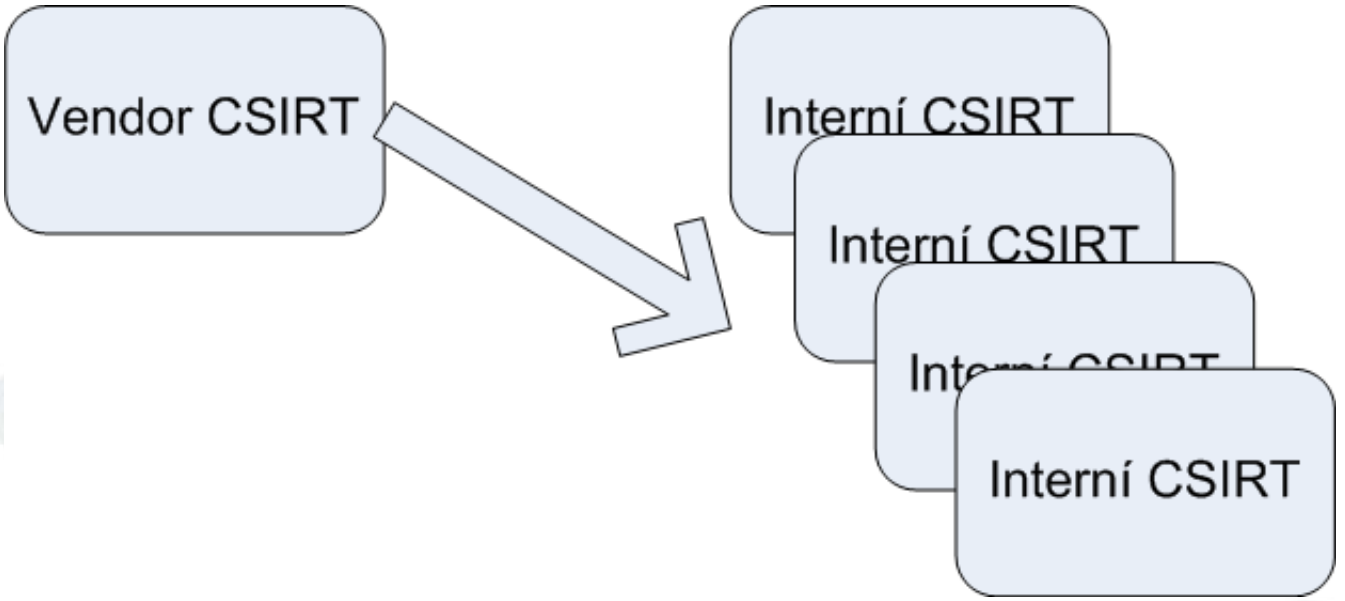
- Use case : ve vaší síti je napadený počítač, vyřešte to
- Typicky 90% komunikace mezi CSIRT týmy

Typy komunikace – II.



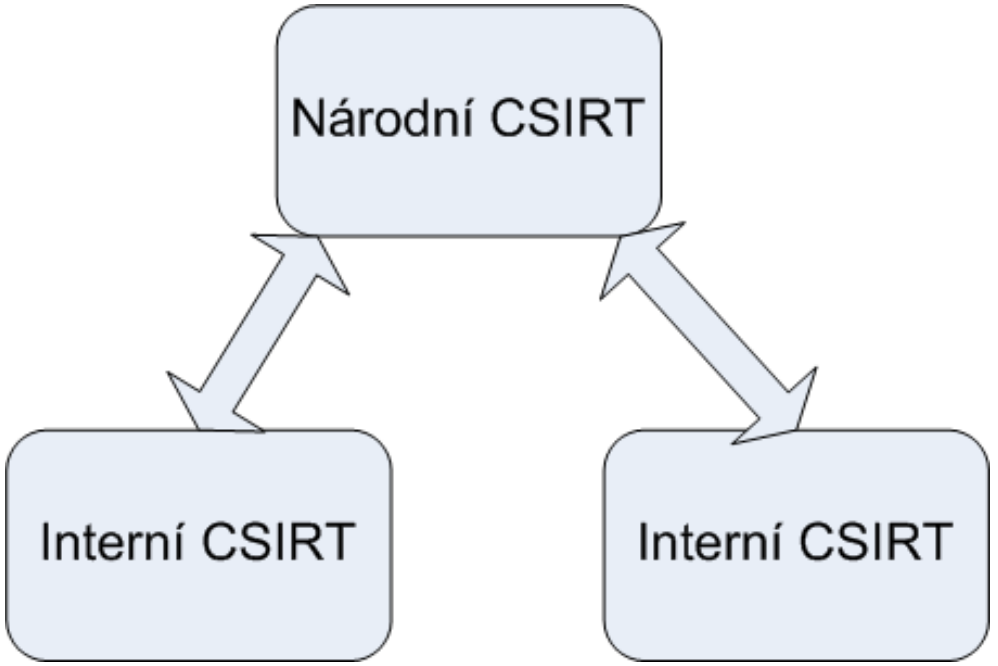
- Jeden (oba) týmy potřebují pomoc odborníka
  - Problémy s routery
  - Chyby v OS, jiném SW, hlášení virů, …

Typy komunikace – III.



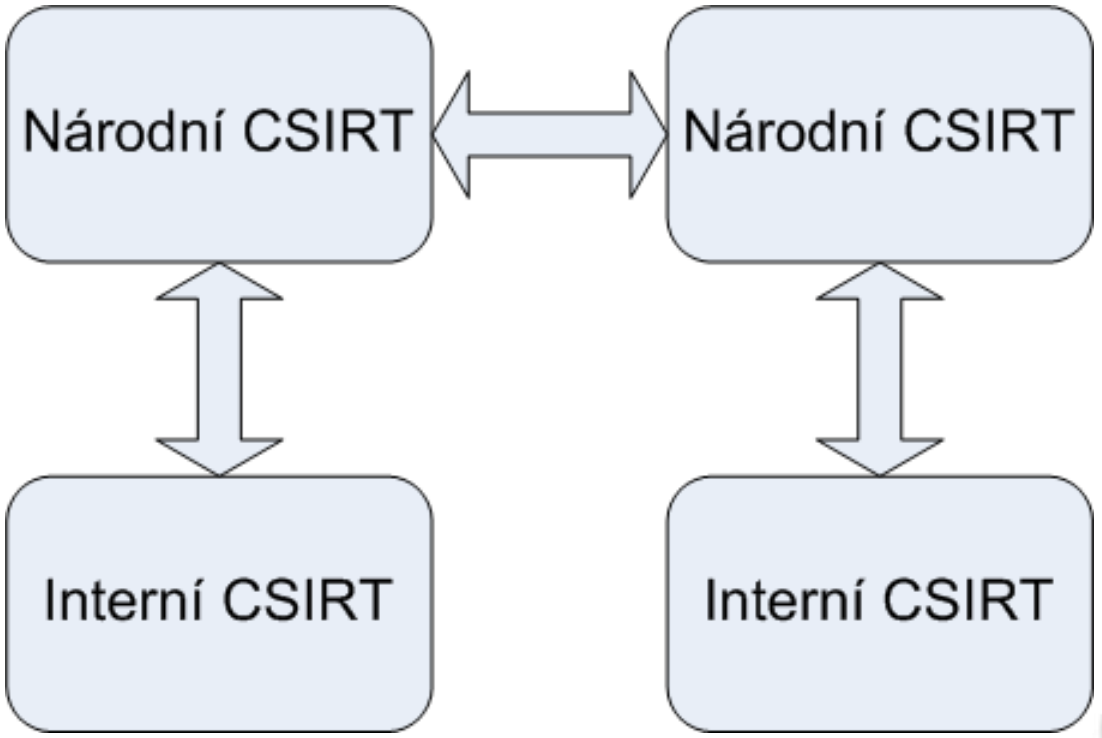
- Odhalení, oprava a komunikování chyby
  - Nemusí být jen směrem k CSIRT týmům

Typy komunikace – IV.



- Use case : někdo na mne útočí, ale nemohu najít příslušnou autoritu
- Komunikaci zprostředkuje národní CSIRT

Typy komunikace – V.



- Use case : někdo na mne útočí, ale nemohu najít příslušnou autoritu
- Komunikaci zprostředkuje národní CSIRT

Organizace

- TERENA
  - Evropská platforma pro vývoj a spolupráci v oblasti internetových technologií
  - http://www.terena.org/

- TF-CSIRT
  - Jedna z aktivit Tereny, sdružuje bezpečnostní týmy
  - http://www.terena.org/activities/tf-csirt/
  - Provozuje službu TI (Trusted Introducer)
    - Členy jsou jednotlivé CSIRT týmy (149 členů)
    - Listed, accredited, certified
    - http://www.trusted-introducer.nl/

Organizace

- ENISA
  - Evropská agentura pro bezpečnost sítí a informací,
  - Zlepšování informační bezpečnost v rámci Evropské unie
  - http://www.enisa.europa.eu/
- FIRST
  - Celosvětové fórum bezpečnostních týmů
  - Cca 250 členů
  - http://www.first.org/
- CERT/CC
  - Koordinační centrum národních a vládních CSIRT týmů
  - http://www.cert.org/certcc.html

CZ.NIC a CSIRT

- CZ.NIC-CSIRT
  - Interní bezpečnostní tým

- CSIRT.CZ
  - Národní CSIRT pro ČR
  - Do 30.6.2012 plní částečně i funkci vládního CSIRT pracoviště

CZ.NIC-CSIRT

- Založen 2008
- Status „akreditovaný“ u TI
- Interní bezpečnostní tým CZ.NIC
  - řešení interních bezpečnostních incidentů
  - právo zrušit delegaci domény při ohrožení (mezi)národní bezpečnosti (na 1 měsíc)
    - škodlivý obsah (malware, viry), phishing, řídící centrum botnetu
- Neřešíme tímto způsobem spamy, ochranné známky, autorská práva apod.

CSIRT.CZ – historie vzniku

- 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

- Memorandum mezi MV ČR a CZ.NIC ze dne 9.12.2010
- http://www.nic.cz/files/nic/doc/Memorandum_CSIRT.CZ.pdf
- CZ.NIC provozuje pracoviště CSIRT.CZ od 1.1.2011

CSIRT.CZ

Komunikace se zahraničím

- TF-CSIRT, TI
  - status „accredited“ přidělen v říjnu 2011
- ENISA
  - Spoluúčast na pořádání 6th CERT workshop (Praha, říjen 2011)
- CERT/CC
  - Účast na výročním zasedání CERT/CC, představení týmu

CSIRT.CZ

Spolupráce v rámci ČR

- Pracovní skupina CSIRT.CZ
  - Pokračování v úspěšné spolupráci
  - Setkání pracovní skupiny v dubnu 2011
  - Připomínkování „Strategie ČR pro oblast kybernetické bezpečnosti“
- Kurz „Svět internetu a domén“
  - Pro pracovníky státní správy, pilotní kurz proběhl v červenci 2011
- Systém vyhodnocování malware a phishing na .cz doménách
  - Spolupráce CZ.NIC Labs, CZ.NIC-CSIRT, CSIRT.CZ
- Proaktivní vyhledávání nezabezpečených DNS
  - Osloveno 1 500 majitelů nezabezpečených serverů
  - Spolupráce s BIS

CSIRT.CZ

Otázky ?
Děkuji za pozornost

CZ.NIC z.s.p.o.
Martin Peterka / martin.peterka@nic.cz
http://www.nic.cz