

Vytvoření a management bezpečnostního týmu

10. května 2007, Blue Room, Karolinum

Andrea Kropáčová

andrea@cesnet.cz

7275 7E6F 39E4 261D FF15 8973 BE2B 53A7 D874 7FE5

Teorie

- Co je bezpečnostní tým?
- Proč potřebujeme bezpečnostní tým?
- Co by měl bezpečnostní tým dělat?
- Jak začít?
- Kolik členů by měl mít bezpečnostní tým?
- Co je potřeba znát?
- Kolik stojí vytvoření a provoz bezp. týmu?
- Jaké jsou základní podmínky?

Realita

- Co je bezpečnostní tým?
- **Proč potřebujeme bezpečnostní tým?**
- **Co by měl bezpečnostní tým dělat?**
- **Jak začít?**
- Kolik členů by měl mít bezpečnostní tým?
- Co je potřeba znát?
- Kolik stojí vytvoření a provoz bezp. týmu?
- Jaké jsou základní podmínky?

Odpověď

- Stávající stav:
 - Správce je “holka pro všechno”
 - Uživatel je bezradný
- Každá organizace (sít') by měla mít jasně definováno následující:
 - Základní pravidla pro hlášení zjištěných bezpečnostních incidentů
 - Komu (na kterou adresu) je možné nahlásit zjištěný bezpečnostní incident
 - Kdo za řešení zjištěných/ohlášených BI zodpovídá

==> tyto informace je nutné zveřejnit a držet aktuální!!!!

Co by měl bezpečnostní tým dělat

- **Představovat záchytný bod pro:**
 - okolní svět (= ostatní bezpečnostní týmy), na který se mohou obracet se žádostí o vyřešení BI
 - uživatele dané sítě, na který se mohou obrátit s podezřením na BI
- **Definovat základní pravidla pro hlášení a řešení BI v dané síti, např.:**
 - Uživatel musí každý BI nebo podezření ohlásit určenému správci a jak
 - Správce musí při řešení BI spolupracovat se členem BT

Jak na to v CESNET2

- Bezpečnostní tým (CSIRT/CERT) může být každá skupina správců, např. příjemci jedné **abuse** adresy
- Stačí jeden základní cíl:
 - Provádět **Incident handling** pro domovskou síť
- Jak začít
 - Určit členy týmu
 - Definovat zodpovědnost
 - Definovat základní pravidla pro IH v dané síti
 - Definovat základní pravidla pro hlášení BI
 - Definovat a zveřejnit základní kontaktní informace

Zveřejnění existence týmu

- **Webová stránka obsahující:**
 - Základní kontaktní informace
 - Pole působnosti
 - Nabízené služby
- Diskusní el. listy
- Lokální zpravodaj
- Konferencích, seminářích, ve výročních zprávách
- Součást info balíčku pro ***nové zaměstnance a studenty***

CESNET-CERTS

- Provozován sdružením CESNET
- Operuje nad sítí CESNET2
- Oficiálně založen v lednu roku 2004
- <http://www.cesnet.cz/csirt>
- CSIRT (Computer Security Incident Response Team)
- Členové:
 - Andrea Kropáčová
 - Pavel Kácha
 - Pavel Vachek
 - Vladimír Třeštík (nováček :-)

CESNET-CERTS

- Přijímáme adresy:
 - abuse@cesnet.cz - hlavní kontakt pro celou CESNET2
 - certs@cesnet.cz
 - ***master*** adresy domén provozovaných CESNET
- Plně zodpovědní za adresové bloky označené jako INFRA-AW v databázi **RIPE**
- Provádíme základní incident handling pro celou síť CESNET2
- Od ledna 2007 základní IH provádí PSS

Štábní kultura CESNET-CERTS

- Systém týdenních služeb:
 - Služba začíná v úterý
 - Pondělí slouží pro:
 - dovyřízení otevřených kauz
 - sepsání reportu o uplynulém týdnu
- Základní IH provádí PSS
- Používáme systém OTRS
 - Šablony podle typu incidentu
 - *Podepisujeme každou odchozí zprávu*

“Incident handling”

- **Chceme odpověď** v případě:
 - Autor stížnosti ji chce nebo by ji uvítal
 - Neřešeného nebo opakujícího se problému
 - V případě závažných incidentů vždy
- **Nechceme odpověď** v případě:
 - Autor stížnosti explicitně napsal, že ji nechce
 - Stížnost (*ojedinělá!!!*) je od automatu (SpamCop, myNetWatchman)

==> můžeme ji chtít my (= CESNET-CERTS)

Role CESNET-CERTS v síti CESNET2

- Pro pohled “zvenku”
 - Hlavní kontakt pro celou CESNET2 - abuse@cesnet.cz
 - “Poslední instance” pro celou CESNET2
 - Záchytný bod pro rezistentní a neřešené problémy
 - Komunikační protějšek pro ostatní světové CSIRT/CERT týmy

Role CESNET-CERTS v síti CESNET2

- Pro pohled “zevnitř” (z CESNET2)
 - Koordinační při řešení BI
 - Záchytný bod pro rezistentní a neřešené problémy
 - Chceme koncovým správcům pomoci, ne je buzerovat!
 - Vzdělávání – semináře, školení, radou ...
 - Odříznutím problematického prvku/sítě
- S čím můžeme také pomoci:
 - S neexistencí adresy pro hlášení BI
 - S nefunkčností adresy pro hlášení BI

Cíle CESNET-CERTS

- Zřízení a provoz bezpečnostního týmu (CSIRT/CERT) v každé síti připojené do sítě CESNET2, obzvláště v těch velkých
- Ustanovit základní komunikační pravidla mezi těmito týmy
- WIRT je živým důkazem, že to jde :-)

?

Otázky

Děkujeme za účast!