cesnet

CERT & CSIRT

Andrea Kropáčová
CESNET

27. 11. 2020
Praha

CERT/CSIRT

- 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***
- PoC dané sítě, místo, 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 incidentů
  - zvyšování bezpečnosti sítě a služeb
- Edukační prvek
  - Pro provozovatele sítí
  - Pro uživatele

CESNET-CERTS

- Provozován CESNET, z. s. p. o.
- https://csirt.cesnet.cz
  - abuse@cesnet,cz, certs@cesnet.cz
- 9 členů - Andrea Kropáčová, Pavel Vachek, Pavel Kácha, Daniel Studený, Jan Mach, Jiří Ráž, Daniel Kouřil, Martin Černý, Václav Bartoš
- Constituency (pole působnosti): AS2852, AS48091
  - vysoké školy, nemocnice (některé), úřady ...
- Zázemí & činnosti
  - řešení a koordinace řešení BI v constituency
  - národní a mezinárodní spolupráce
  - vývoj aplikací pro zjednodušení práce – OTRS, Negistry
  - vývoj systémů pro zpracování informací z bezpečnostních nástrojů – Warden & Mentat
  - účast v národních a mezinárodních projektech
  - vzdělávání (semináře, školení, osvětové akce)

- Výkonný & koordinační
- Výkonný
  - pro adresové rozsahy vlastní infrastruktury (páteře, serverových segmentů, lokálních sítí...)
  - může být represivní – vypnout stroj, zablokovat, zafiltrovat
  - úzká spolupráce se správci sítě a služeb (vlastní zaměstnanci)
- Koordinační
  - pro AS2852, AS48091
  - může být represivní jen prostředky uplatnitelnými na hraně sítě (filtr, FW, QoS), nemůžeme „vypnout zařízení“ v připojené instituci
  - může radit, koordinovat, poskytnout svůj díl informací k danému problému
- Incident Handling proces má mnoho aspektů
  - technický
  - politický
  - legislativní
  - ... na všechny je potřeba být připraven!

cesnet

SOC

Security Operations Centre

... zajišťuje komplexní centralizaci řízení bezpečnostních událostí a incidentů v jednom bodě s cílem minimalizovat reakční doby na incident a škod z něj plynoucích. Bezpečnostní operační centrum stojí na pilířích přípravy, detekce, analýzy, investigace, reakce a post incident aktivit ...

SOC v CESNET

- SOC v CESNET je distribuovaný a tvoří jej následující kooperující jednotky

- **CESNET-CERTS**
  - bezpečnostní tým pro dohled nad e-infrastrukturou CESNET
- **Forenzní laboratoř** (flab.cesnet.cz)
  - analýza bezpečnostních incidentů, penetrační a zátěžové testy
- **NOC** (Network Operation Centre)
  - správa páteřní sítě CESNET2, 24/7
- **PSS** (Pracoviště stálé služby)
  - dohledové pracoviště, 24/7
- **Správci služeb**

SOC v CESNET

- SOC v CESNET je distribuovaný a tvoří jej následující kooperující jednotky

- **CESNET-CERTS**
  - bezpečnostní tým pro dohled nad e-infrastrukturou CESNET
- **Forenzní laboratoř** (flab.cesnet.cz)
  - analýza bezpečnostních incidentů, penetrační a zátěžové testy
- **NOC** (Network Operation Centre)
  - správa páteřní sítě CESNET2, 24/7
- **PSS** (Pracoviště stálé služby)
  - dohledové pracoviště, 24/7
- **Správci služeb**
- **Monitoring e-infrastruktury a služeb**
  - perimetru
  - na bázi netflow, snmp
  - Nagios
  - sběr informací o BI a BÚ, zranitelností ...

SOC v CESNET

- SOC v CESNET je distribuovaný a tvoří jej následující kooperující jednotky

- **CESNET-CERTS**
  - bezpečnostní tým pro dohled nad e-infrastrukturou CESNET
- **Forenzní laboratoř** (flab.cesnet.cz)
  - analýza bezpečnostních incidentů, penetrační a zátěžové testy
- **NOC** (Network Operation Centre)
  - správa páteřní sítě CESNET2, 24/7
- **PSS** (Pracoviště stálé služby)
  - dohledové pracoviště, 24/7
- **Správci služeb**
- **Monitoring e-infrastruktury a služeb**
  - perimetru
  - na bázi netflow, snmp
  - Nagios
  - sběr informací o BI a BÚ, zranitelností ...

Detekce

Analýza

Reakce

Náprava

Poučení

cesnet

Use-cases

Use-case: phishing

- Provedení: vlna podvodných mailů s malwarem (s URL s malware), který po uhnízdění v počítači zařízení zařadí do botnetu

Use-case: phishing

- Včasná detekce
  - v antispam ochraně
  - v doméně
  - poučený uživatel
- Zkomplikovat další příjem
  - specifický spamfiltr
- Zkomplikovat malware spuštění
  - smazat z e-mailových schránek
  - konkrétní pravidla v HIPS/AV řešení
  - informovat uživatele
- Minimalizovat dopady
  - Zakázat odchozí poštu na „reply-to“
  - Blokovat URL pro podvržené stránky
  - Blokovat na perimetru spojení s IP C&C / dropzóny

Use-case: phishing

- Identifikovat kompromitované stanice
  - Lokálně (souborový systém, registry)
  - Podle síťového provozu
- Identifikovat dopady kompromitace
  - Lokální
    - Odchycení hesel, uložená data (změna, smazání, krádež)
  - „Dosah“ mimo pracovní stanici
    - Změny v informačních systémech
  - Šíření přes úložiště (např. Cryptolocker a namapované disky)
- Návrat do normálu
  - vylepšení ochrany
  - poučení uživatelů

Use-case: phishing

- Role organizace (cíle útoku)
- Role CESNET (jako připojovatele, operátora)

Use-case: phishing

Může CESNET připojené instituci nějak pomoci?

- Včasná detekce
  - v antispam ochraně
  - v doméně
  - poučený uživatel

Jen za určité situace (např. kampaň je rozsáhlá)

- Zkomplikovat další příjem
  - specifický spamfiltr

Částečně
- analýza mailu

- Zkomplikovat malware spuštění
  - smazat z e-mailových schránek
  - konkrétní pravidla v HIPS/AV řešení
  - informovat uživatele

Částečně
- analýza malware

- Minimalizovat dopady
  - Zakázat odchozí poštu na „reply-to“
  - Blokovat URL pro podvržené stránky
  - Blokovat na perimetru spojení s IP C&C / dropzóny

NE
Možná
ANO

Use-case: phishing

Může CESNET připojené instituci nějak pomoci?

- Identifikovat kompromitované stanice
  - Lokálně (souborový systém, registry)
  - Podle síťového provozu

NE
Možná

- Identifikovat dopady kompromitace
  - Lokální
    - Odchycení hesel, uložená data (změna, sm
  - „Dosah“ mimo pracovní stanici
    - Změny v informačních systémech
  - Šíření přes úložiště (např. Cryptolocker a namapované disky)

Částečně

- Návrat do normálu
  - vylepšení ochrany
  - poučení uživatelů

Částečně

- doporučení
- školení uživatelů

Poučení

- Bezpečnost v naší organizaci za nás nikdo neudělá
- Bezpečnost nelze outsourcovat

Use-case: útok zevnitř

- Připojená organizace se stane zdrojem útoku
- Detekce – analýza – reakce – náprava - ...
- Role organizace
  - detekce
  - analýza - pro prvotní reakci, identifikace příčiny
  - zásahy v síti (FW, filtry ...)
  - eliminovat zdroj problému (např. dohledání a deaktivace zdrojů)
- Role CESNETu jako operátora
  - detekce
  - analýza
  - reakce = nasadit obranu na perimetru
  - pomoc připojené instituci např. s analýzou, návrhem řešení
- Obě strany
  - spolupráce, komunikace
  - připravenost

Poučení

- Bezpečnost v naší organizaci za nás nikdo neudělá
- Bezpečnost nelze outsourcovat
- Připravenost
  - znám svou organizaci a její potřeby
  - vím, co je potřeba chránit
  - vím, co pro mě dokáže udělat partner (poskytovatel připojení)
  - vím, kam se obrátit

K diskusi ...

- Každý vlastní CSIRT a společná úzká platforma – klub?
  - ala aktivity Vládního a Národního CERT/CSIRT

- Společný CSIRT pro nemocnice?
  - zdroj know-how
  - vytěžení a distribuce informací
  - doporučení
  - koordinace komunikace v případě krizových situací

- Co jsme ochotni sdílet? Do jaké míry?
  - informace?
  - zdroje?
  - lidi?

Děkuji za pozornost.

Andrea Kropáčová

andrea@cesnet.cz