Seminář o bezpečnosti sítí a služeb

11. února 2015

CESNET, z. s. p. o.

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

2007–13
OP Výzkum a vývoj pro inovace

CESNET, z. s. p. o.

- Založen v roce 1996
- Členové
  - 25 českých univerzit
  - Akademie věd České republiky
  - Policejní akademie ČR
- Hlavní cíle:
  - výzkum a vývoj informačních a komunikačních technologií
  - budování a rozvoj e-infrastruktury CESNET určené pro výzkum a vzdělávání
  - podpora a šíření vzdělanosti, kultury a poznání
- **2011 – 2015**
  - **Projekt Velká infrastruktura CESNET**

Rámcový pohled na e-infrastrukturu a její služby

Bezpečnostní školení

Řešení bezpečnostních incidentů (CSIRT)

Uživatelská podpora, dohled, monitoring

DNS služby, záložní poštovní služby

Prostředí pro vývoj a testování (PlanetLab)

Projektování fotonických systémů a sítí

Realizace jednorázových akcí (dema, přenosy, ...)

Poskytování licencí k výsledkům VaV

Snadný přístup k síťovým službám v rámci komunity - eduID.cz

Certifikáty pro uživatele a servery

Federovaný přístup k síti - eduroam

Správa identit, PKI & AAI

Sledování infrastruktury a provozu sítě

Monitorování kvalitativních charakteristik sítě

Datová úložiště

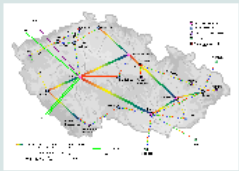
MetaCentrum NGI

Podpora spolupráce uživatelů

Technické konzultace

Časové služby

Cisco akademie



Společná komunikační Infrastruktura

Prostředí pro zálohování, archivaci, sdílení dat

Úložiště dat pro speciální aplikace

Úschovna dat - FileSender

Lambda služby

Fotonické služby

Náročné výpočetní a datové služby

Integrace výpočetních kapacit

Koordinace pořizování a správy programového a aplikačního vybavení

Přidělování adresových zdrojů

Zřízení vyhrazených okruhů a sítí

Připojení internetovým protokolem

Videokonference, Webkonference, IP telefonie

Streaming

Foodle

Videoarchiv

Speciální obrazové přenosy

Bezpečnost a Česká republika 2015

Andrea Kropáčová, andrea@cesnet.cz
CESNET, z. s. p. o.

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI
2007–13
OP Výzkum a vývoj pro inovace

CERT/CSIRT v ČR

16 + *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)
- *FORPSI-CSIRT (CSIRT tým společnosti INTERNET CZ, a. s.)*
- *KAORA, s.r.o.*

Vládní a Národní tým

- **GovCERT.CZ** (Vládní CERT), http://www.govcert.cz/
  - provozován NBÚ
    - gestor za oblast kyberbezpečnosti z pověření vlády ČR (2011)
  - pole působnosti: sítě státní správy a samosprávy, kritická infrastruktura
  - „Listed" od 2013, „accredited" od srpna 2014

- **CSIRT.CZ** (Národní CSIRT), http://www.csirt.cz/
  - provozován sdružením CZ.NIC
    - Memorandum mezi MV ČR a CZ.NIC ze dne 9.12. 2010
    - Memorandum mezi NBÚ a CZ.NIC ze dne 1.4.2012
  - pole působnosti: Česká republika
  - „Listed" od 2008, „accredited" od 2011

CERT/CSIRT v ČR

- 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)
- *FORPSI-CSIRT (CSIRT tým společnosti INTERNET CZ, a. s.)*
- *KAORA, s.r.o.*

Vrcholové týmy
–
Národní a Vládní

CERT/CSIRT v ČR

- 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)
- *FORPSI-CSIRT (CSIRT tým společnosti INTERNET CZ, a. s.)*
- *KAORA, s.r.o.*

Týmy působící v akademickém prostředí

CERT/CSIRT v ČR

- 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)
- *FORPSI-CSIRT (CSIRT tým společnosti INTERNET CZ, a. s.)*
- *KAORA, s.r.o.*

Týmy působící v sítících významných ISP

CERT/CSIRT v ČR

- 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)
- *FORPSI-CSIRT (CSIRT tým společnosti INTERNET CZ, a. s.)*
- *KAORA, s.r.o.*

Týmy na půdě významných provozovatelů služeb

CERT/CSIRT v ČR

- 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)
- *FORPSI-CSIRT (CSIRT tým společnosti INTERNET CZ, a. s.)*
- *KAORA, s.r.o.*

Týmy působící v bankovním sektoru

Projekt Fenix

- http://fe.nix.cz/
- Projekt českého peeringové centra NIX.CZ, http://www.nix.cz/
- Odpověď na (D)DoS útoky z 3/2013
  - 4 dny, dvě vlny, metody SYN-Flood, IP-Spoofing, „reflection“
  - mnoho cílů v CZ (média, banky, mobilní operátoři, Seznam.cz)
  - zdroj útoků mimo CZ, via NIX.CZ
- Cíl: *„CZ uživatelé se potřebují dostat na CZ zdroje“*
  - možnost fungování v ostrovním režimu jako poslední možnost
- Přísná kritéria pro vstup: organizační, technická
- Klub vzájemně „důvěryhodných“ (aktuálně 9 členů)
  - NIX.CZ, CZ.NIC, O2, CESNET, Dial Telecom, Active24, Coolhousing, ČD- Telematika, Casablanca

ZKB

- **Zákon** č. 181/2014 Sb., **o kybernetické bezpečnosti** a o změně souvisejících zákonů (ZKB)
  - tvorba od prosince 2011, NBÚ
  - platný od srpna 2014
  - účinný od 1. ledna 2015
- Prováděcí předpisy k ZKB (17. prosince 2014)
  - Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)
  - Vyhláška, **kterou se stanoví významné informační systémy a jejich určující kritéria**
  - Novela nařízení vlády č. 432/2010 Sb., **o kritériích pro určení prvku kritické infrastruktury**
- **Dokumenty** viz stránky – www.nbu.cz, www.govcert.cz

§ 3 ZKB

- Orgány a osoby, kterým se ukládají povinnosti v oblasti kybernetické bezpečnosti:

  a) poskytovatel služby elektronických komunikací a subjekt zajišťující **síť elektronických komunikací**, pokud není orgánem nebo osobou podle písmene b),

  b) orgán nebo osoba zajišťující **významnou síť**, pokud nejsou správcem komunikačního systému podle písmene d),

  c) správce informačního systému kritické informační infrastruktury,

  d) správce komunikačního systému kritické informační infrastruktury a

  e) správce významného informačního systému.

- Pojem **významná síť** (dle § 2 ZKB) je definován tak, aby zahrnoval síť elektronických komunikací zajišťující **přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé připojení ke kritické informační infrastruktuře**.

§ 3 ZKB písmeno a)

Základní povinnosti	**Povinnosti – stav kybernetického nebezpečí**
- hlásit kontaktní údaje národnímu CERT *(oznámí kontaktní údaje podle § 16 nejpozději do 30 dnů ode dne nabytí účinnosti tohoto zákona)*	- provádět reaktivní opatření vydaná NBÚ za stavu kybernetického nebezpečí nebo za nouzového stavu (Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky, ve znění ústavního zákona č. 300/2000 Sb.) - Možnost uplatnění rozhodnutí nebo opatření obecné povahy podle § 13 - Kontrola ze strany NBÚ, jak jsou tato opatření prováděna.

§ 3 ZKB písmeno b)

Základní povinnosti	**Povinnosti – stav kybernetického nebezpečí**
- hlásit kontaktní údaje národnímu CERT *(oznámí kontaktní údaje podle § 16* ***nejpozději do 30 dnů ode dne nabytí účinnosti tohoto zákona)*** - detekovat kybernetické bezpečnostní události - hlásit kybernetické bezpečnostní incidenty národnímu CERT *(tuto povinnost začnou plnit nejpozději do 1 roku ode dne nabytí účinnosti ZKB – tj. 1.1.2016)*	Hlásit kontaktní údaje národnímu CERT, detekovat kybernetické bezpečnostní události, hlásit kybernetické bezpečnostní incidenty národnímu CERT, **provádět reaktivní opatření vydaná NBÚ**

CESNET-CERTS

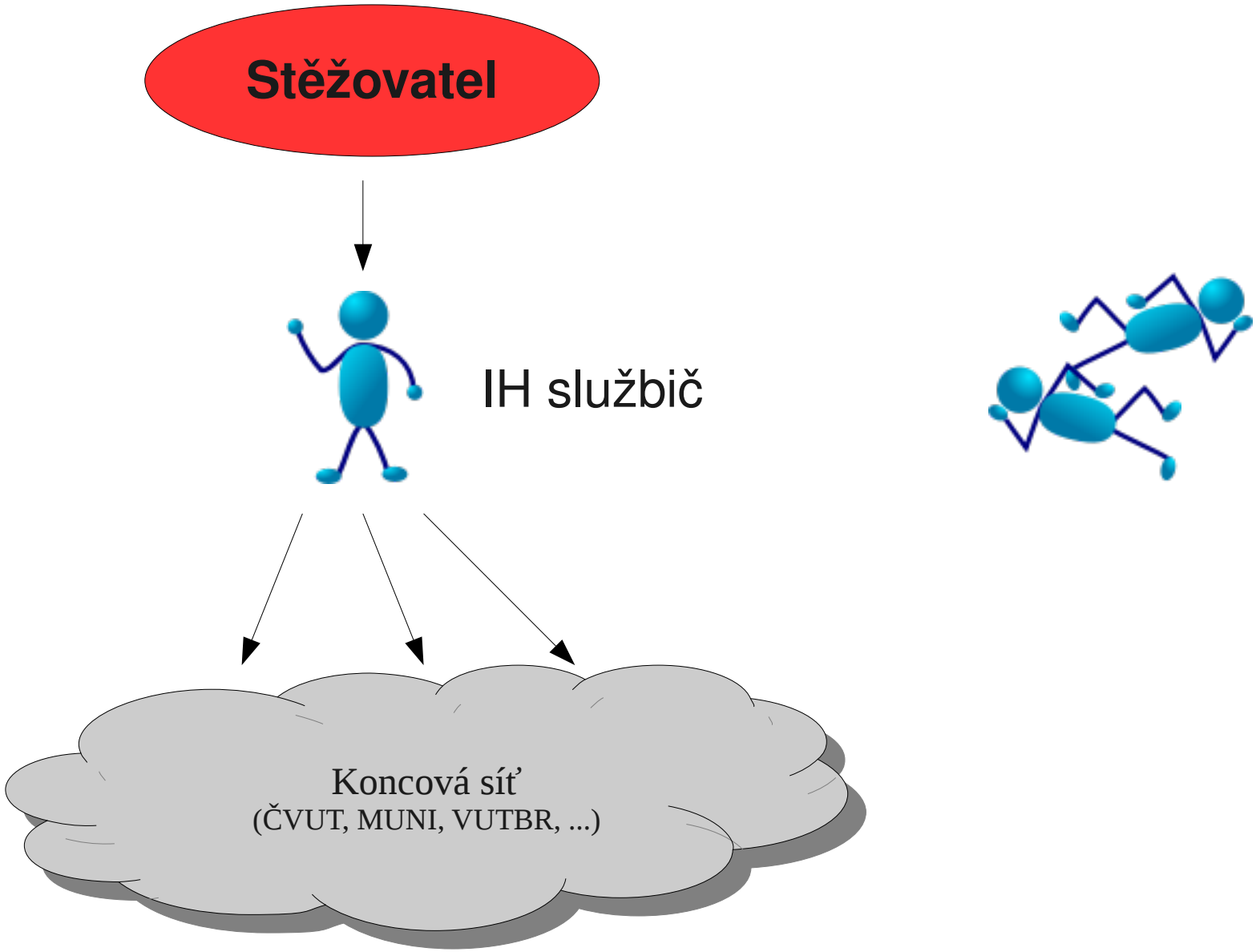
- http://csirt.cesnet.cz, certs@cesnet.cz, abuse@cesnet.cz
- 341D 3EB0 0160 941F 6A06 4401 F9BF C741 9CAA 8579
- +420 2 2435 2994

- Provozován sdružením CESNET
- Pole působnosti – CESNET2 (AS2852)
- Koordinační + interní tým
- Vznik 2003, „listed“ 2004, „accredited“ v roce 2008
- 3 ... 4 ..... 7 9

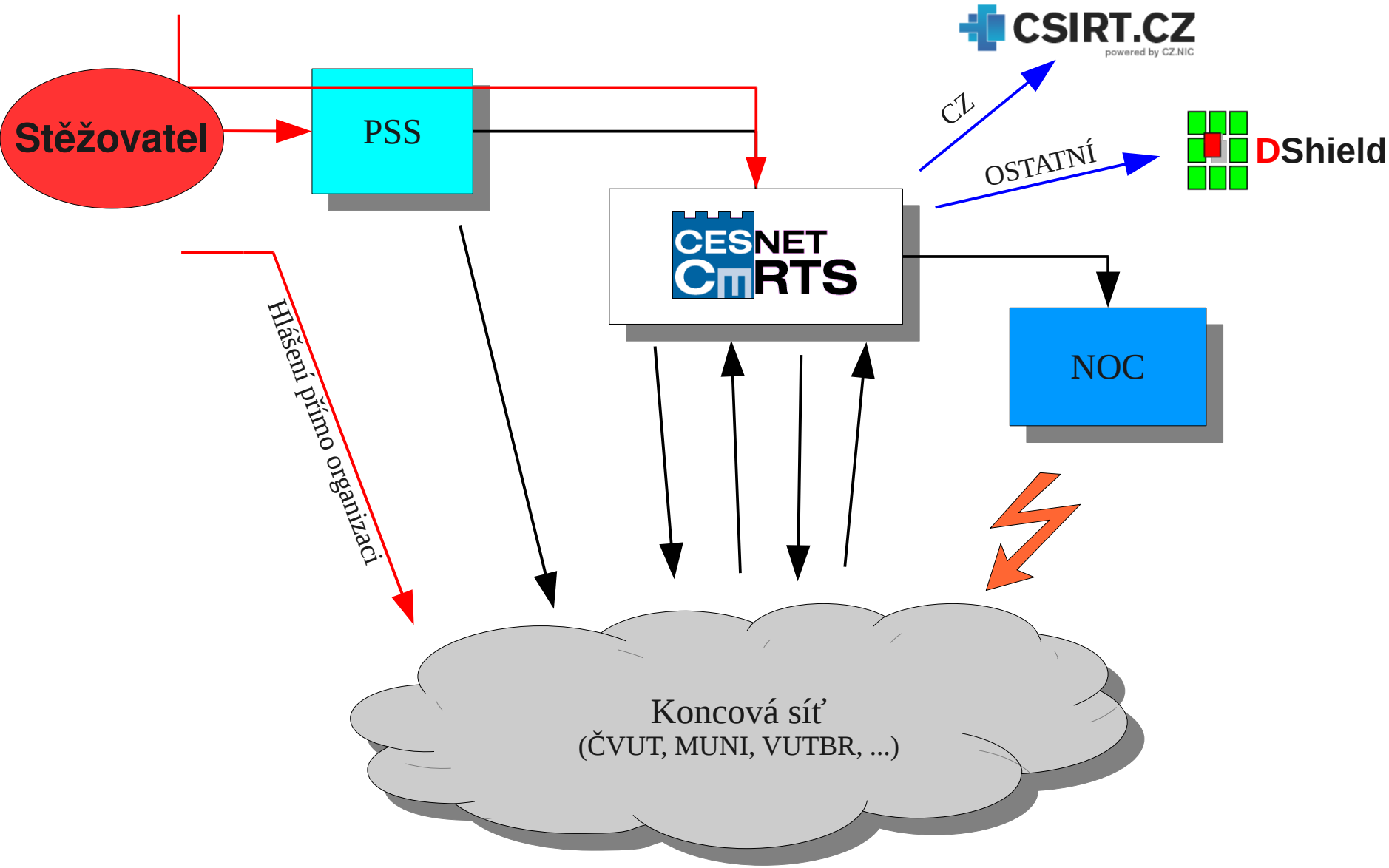
Tři zakládající členové (rok 2003):

- Andrea Kropáčová
- Pavel Vachek
- Pavel Kácha

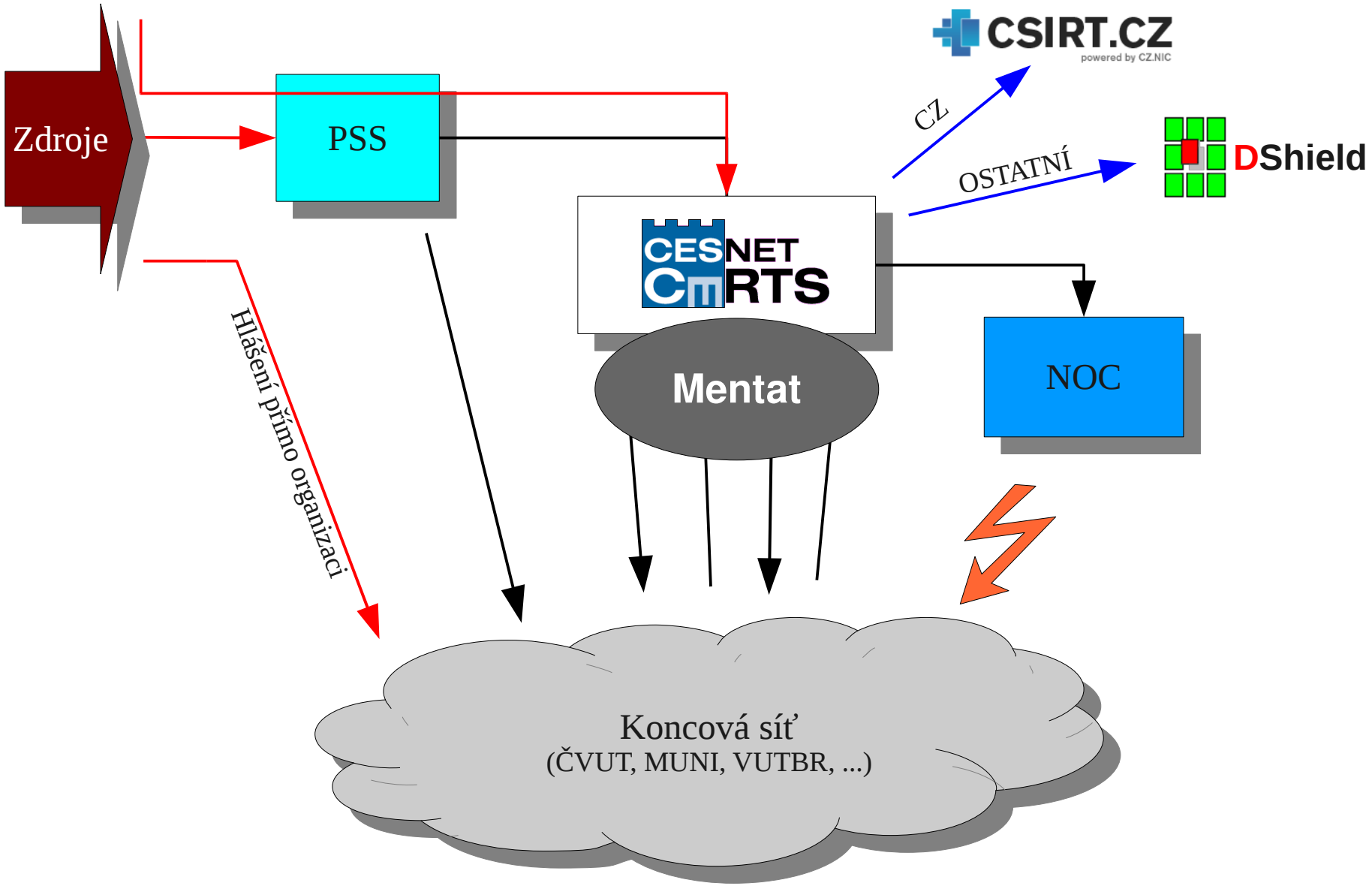
Proces incident handling a incident response v roce 2004



Vývoj procesu incident handling a incident response v 2004 ... 2015

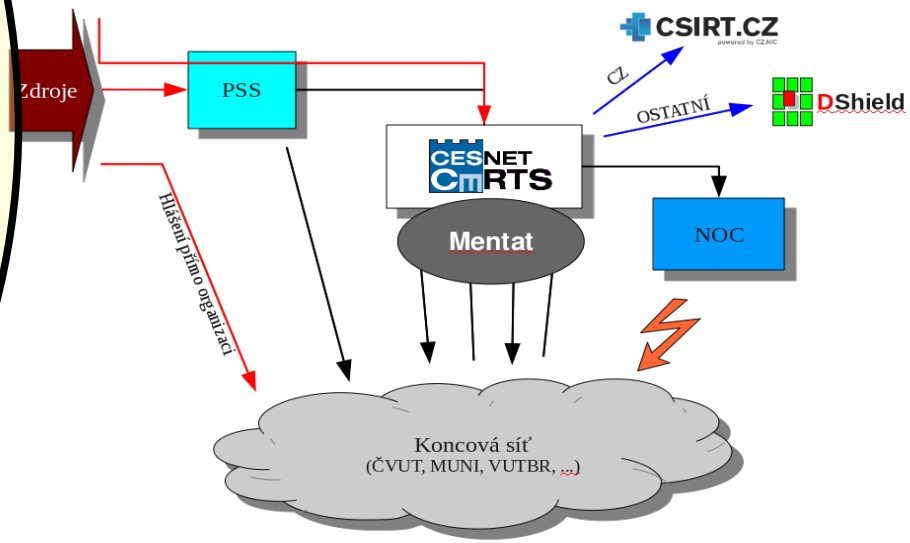


Vývoj procesu incident handling a incident response v 2004 ... 2015



Rok 2015

=



Zdroje informací o dění v síti CESNET2 – IDS, honeypoty, FW, netflow, sondy, logy, zdroje třetích stran ...

Služby CESNET-CERTS

- Řešení a koordinace řešení bezpečnostních incidentů
  - sběr, vyhodnocení a distribuce dat do koncových sítí
- Pomoc při zvládání bezpečnostních incidentů
  - zásahem v síťové infrastruktuře ve spolupráci s NOC
  - ověřením v bezpečnostních nástrojích (sondy, FTAS, G3)
  - testování (HeartBleed, Shellshock), audit
- Služby na bázi sdílení a rozvoje komunity (dáš, dostaneš)
  - Warden, http://warden.cesnet.cz/
- Služby FLAB
  - forenzní analýza
  - penetrační testy, testy odolnosti

Další služby

- STaaS (Security Tools as a Service)
  - služba pro členy, jejichž možnosti v oblasti bezpečnosti jsou omezené
  - aplikace zkušeností z CESNET2 do menších sítí
  - nasazení a vyladění monitorovacích nástrojů pro konkrétní síť
    - zprovoznění sondy, instance FTAS, G3
    - možnost provozovat vlastní instanci služby s podporou CESNETu, nebo využít instanci CESNETu a mít přístup k výsledkům
    - konzultace a vzdělávání, práce s nasbíranými daty
- Antispam Gateway (aka „pračka elektronické pošty“)
- Diseminace
  - školení (upcoming DNS)
  - semináře, pracovní skupina
  - prezentování

Strategie v oblasti bezpečnosti

I. Udržet e-infrastrukturu CESNET v běhu a zabezpečenou

II. Zvyšovat v oblasti bezpečnosti schopnosti připojených institucí

III. Ochrana a vzdělávání uživatelů

Naplňování strategie

- **Vyvíjíme a provozujeme nástroje, technologie a služby které:**
  - podají obraz o dění v síti
  - detekují anomálie (podezřelé chování) v provozu sítí a služeb
  - dovolí zaměřit se na podezřelý provoz
  - umožní sdílení zajímavých dat
  - informace o anomáliích (události, BI) dostanou do rukou správců

    ==> aktivní obrana

    ==> „zdravotní aspekt“, prevence

  - **umožní detekci, sběr, analýzu a vytěžení těchto dat**
  - **umožní vyhodnocení, zpracování a nápravu**

Bezpečnostní infrastruktura

- **Síťové sondy** na perimetru sítě CESNET2
- **FTAS a G3**
  - plošné souvislé sledování IP provozu rozsáhlých síťových infrastruktur
  - plošné souvislé sledování stavu a chování rozsáhlých výkonných infrastruktur
- **IDS systémy, Honeypoty**
- **Systémy pro sdílení a korelaci dat**
  - Warden
  - Mentat
- **Forenzní laboratoř** (FLAB)

  - forenzní analýza
  - penetrační testy, testy odolnosti
- **CESNET-CERTS, Pracoviště stálé služby, skupina NOC** (správa páteřní sítě)

Děkuji za pozornost.