Bezpečnost

Andrea Kropáčová

Program

- **Aktuální stav a trocha bezpečnostní historie v provozu i výzkumu** *(Andrea Kropáčová & Jan Kořenek, CESNET)*
- **Forenzní laboratoř FLAB** *(Aleš Padrta & Michal Kostěnec, CESNET)*
- **Use-cases z bezpečnostního monitoringu e-infrastruktury CESNET** *(Tomáš Košňar & Martin Žádník & Vašek Bartoš, CESNET)*
- **Infrastruktura pro plošný sběr, zpracování a distribuci bezpečnostních událostí – služby Warden, Mentat, DNS, NERD** *(Pavel Kácha, CESNET)*
- **Vize v oblasti bezpečnosti** *(Andrea Kropáčová & Tomáš Košňar & Jan Kořenek & Tomáš Čejka, CESNET)*

Trocha historie I

- **1998:** Základy bezpečnostního monitoringu (dnešní FTAS)
- **2003:** Začínáme s čertěním, jedeme do Varšavy na školení, zakládáme CESNET-CERTS
- **2004:** Komunita nás přijala, TI udělil týmu CESNET-CERTS status *listed*
- **2007:** Projekt „Problematika kybernetických hrozeb z hlediska bezpečnostních zájmů České republiky", 2007 – 2010. Etablujeme CSIRT.CZ.
- **2008:** Akreditujeme CESNET-CERTS a získáváme status *listed* pro CSIRT.CZ
- **2011:** Transferujeme CSIRT.CZ do CZ.NIC, už v roli **Národní CSIRT ČR**
- **2011:** Začínáme budovat FLAB
- **2012:** Začínáme hrátky s daty a automatizací ... Warden, Mentat
- **2013:** Pouštíme pilot Wardenu, máme 22 datových zdrojů ...

Trocha historie II

- **2014:** Otevíráme FLAB, stáváme se členy projektu FENIX
- **2015:** CESNET jako povinný subjekt ZKB, zavádění ISMS
- **2016:** SABU, PROTECTIVE, CTI ...
- **2017:** root.cz – Postřehy z bezpečnosti, první The Catch
- **2018:** Certifikace ISMS
- **2019:** PassiveDNS, NERD

FLAB openning :-)

Trocha historie II

- **2014:** Otevíráme FLAB, stáváme se členy projektu FENIX
- **2015:** CESNET jako povinný subjekt ZKB, zavádění ISMS
- **2016:** SABU, PROTECTIVE, CTI ...
- **2017:** root.cz – Postřehy z bezpečnosti, první The Catch
- **2018:** Certifikace ISMS
- **2019:** PassiveDNS, NERD

CESNET-CERTS

- CESNET-CERTS, csirt.cesnet.cz
- AS2852
- abuse@cesnet.cz, certs@cesnet.cz
- Zázemí & činnosti
  - řešení a koordinace řešení bezpečnostních incidentů
  - národní a mezinárodní spolupráce
  - vývoj aplikací pro zjednodušení práce – OTRS, Negistry
  - vývoj systémů pro zpracování informací z bezpečnostních nástrojů
  - účast v národních a mezinárodních projektech
  - vzdělávání (semináře, školení, osvětové akce)

Andrea Kropáčová

Pavel Vachek

Pavel Kácha

Daniel Studený

Jan Mach

Jiří Ráž

Daniel Kouřil

Martin Černý

Václav Bartoš

Certificate of Accreditation

This certificate is granted by the Authority of the
Trusted Introducer for CSIRTs in Europe (TI) to certify that

CESNET-CERTS

has been registered as "TI Accredited CSIRT" since 27 January 2008.
Consult https://tiw.trusted-introducer.nl/ for team-specific information.

This certificate is valid from 27 January until 31 December 2008 (unless revoked).

TRUSTED Introducer

2008

TERENA

Don Stikvoort
TI Manager


Certificate of Accreditation
CESNET-CERTS
TRUSTED
TERENA

CESNET-CERTS

- CESNET-CERTS, csirt.cesnet.cz
- AS2852
- abuse@cesnet.cz, certs@cesnet.cz
- Zázemí & činnosti
  - řešení a koordinace řešení bezpečnostních incidentů
  - národní a mezinárodní spolupráce
  - vývoj aplikací pro zjednodušení práce – OTRS, Negistry
  - vývoj systémů pro zpracování informací z bezpečnostních nástrojů
  - účast v národních a mezinárodních projektech
  - vzdělávání (semináře, školení, osvětové akce)

Andrea Kropáčová

Pavel Vachek

Pavel Kácha

Daniel Studený

Jan Mach

Jiří Ráž

Daniel Kouřil

Martin Černý

Václav Bartoš

Služby

- CESNET-CERTS, csirt.cesnet.cz
- Bezpečnostní monitoring: FTAS, G3, ExaFS, Warden, Mentat, PassiveDNS, NERD
- Forenzní laboratoř FLAB
- Osvěta, vzdělávání, výměna know-how
  - Semináře o bezpečnosti
  - csirt-forum@cesnet.cz
  - Školení – FA1, FA2, školení základní počítačové gramotnosti
  - individuální konzultace
  - The Catch *... kdo si hraje, vzdělává se...*

Bezpečnostní monitoring

Co sledujeme:

- perimetr sítě, vstup, výstup
- IP provoz v páteři
- provoz „od nás ven“
- podvrhávání zdrojových adres
- provoz vybraných prvků infrastruktury
- klíčové služby (DSN, AAI)
- skenování portů
- synflood útoky
- útoky hrubou silou na ssh, SIP, DNS tunely
- DNS, NTP, SNMP amplifikace
- anomální datové přenosy, paketové rychlosti
- ... „on-demand“ ...

Informační využití:

- informace o uskutečněném provozu
- automatická detekce anomálií
- on-the-fly detekce útoků
- odhalení podvržení adres
- verifikace, analýza bezpečnostních incidentů
- odhalení kompromitovaných zařízení
- vzorky dat, ladění sítě
- obrana sítě, služeb a uživatelů
- systematické sledování provozu instituce
- náhled na provoz sítě
- zdraví, vytížení sítě
- architektura sítě, její optimalizace a rozvoj
- statistiky provozu

Služby

- CESNET-CERTS, csirt.cesnet.cz
- Bezpečnostní monitoring: FTAS, G3, ExaFS, Warden, Mentat, PassiveDNS, NERD
- Forenzní laboratoř FLAB
- Osvěta, vzdělávání, výměna know-how
  - Semináře o bezpečnosti
  - csirt-forum@cesnet.cz
  - Školení – FA1, FA2, školení základní počítačové gramotnosti
  - individuální konzultace
  - The Catch *... kdo si hraje, vzdělává se...*

Spolupráce

- TF-CSIRT
- Národní tým CSIRT.CZ, CZ.NIC
- Vládní CERT
- Fenix, NIX
- Kraj vysočina, E-CRIME
- ...

Děkuji za pozornost!

Andrea Kropáčová

andrea@cesnet.cz