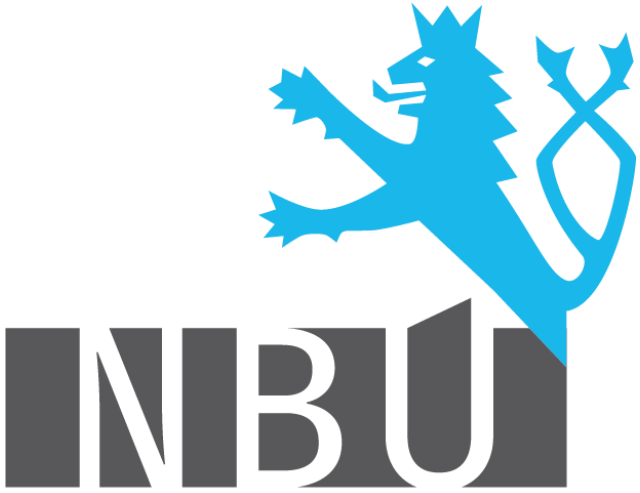

Národní
bezpečnostní
úřad

Národní centrum kybernetické bezpečnosti

NCKB/GovCERT.CZ a další spolupracující CERT a bezpečnostní týmy

Ondřej Šrámek

Obsah prezentace

- Základní **informace** o NCKB/GovCERT.CZ;
- **Národní** a **mezinárodní** spolupráce.

Základní informace 1/2

- Národní centrum kybernetické bezpečnosti;
  - Zřízeno na základě usnesení vlády č. 781 (19. 10. 2011);
- OTPVV;
  - Teoretická podpora;
  - Vzdělání a výzkum;
  - Určování VIS a KII;
- GovCERT.CZ;
  - Reaktivní oddělení;
  - Proaktivní oddělení;
  - Vyhledávací oddělení.

Základní informace 2/2

- CERT: Computer Emergency Response Team;
- Veřejný sektor a kritická informační infrastruktura;
- Členění týmu:
  - Reaktivní oddělení;
  - Oddělení vyhledávání;
  - Analytické oddělení;
- Základní služby:
  - Proaktivní: koordinační činnost v rámci komunity a informační HUB, schopnosti detekce anomálií;
  - Reaktivní: reakce na incidenty, zpracování artefaktů;
- Kontakt:
  - http://www.govcert.cz;
  - cert.incident@nbu.cz (PGP);
  - cert@nbu.cz (PGP).

Národní a mezinárodní spolupráce

Koordinační činnost

- Rozsáhlé útoky (březen 2013)
- Cvičení (Locked Shields, Cyber Coalition, Cyber CZECH,…)

- CSIRT/CERT týmy, bezpečnostní týmy, ostatní subjekty

- Kolaborativní prostředí
  - Připravovaná VZ

Reportování

- Vážný problém;
  - Zasažení většího počtu uživatelů/systémů v ČR (předání informací CSIRT.CZ);
  - Zasažení uživatelů/systémů státní správy/KII/VIS;

  - Distribuce informací k potencionálním obětem/správcům;
  - Pomoc/opatření;
- Selhání všech ostatních pokusů o vyřešení;
  - Pomoc s kontaktem,…

Spolupráce

- Národní PoC;
  - Zprostředkování kontaktu (AV, zahraniční hosting,…);
  - Předání informací (artefakty,...);
- Výměna informací;
  - TLP protokol (red, yellow, green a white);
  - PGP;
- Distribuce informací;
  - Spolupracující CSIRT/CERT týmy;
  - AV společnosti;
  - Vlastní zdroje (OSINT).

Proaktivní činnost

- Botnet Feed;
  - Nástroj vyvíjený za účelem sběru a zpracování dat o koncových uzlech zapojených do botnetů;
  - Záznamy obsahují IP adresy nakažených strojů v ČR;
  - Cca 250 000 záznamů denně;
- Incident Handling Automation Project;
  - Data od bezpečnostních týmů, velkých společností, univerzit a výzkumných laboratoří (indikátory kompromitace);
  - Záznamy obsahují IP adresy reportovaných strojů;
  - Cca 7 000 záznamů denně;
- OSINT;
  - Sběr informací z otevřených zdrojů;
  - Distribuce relevantních informací k subjektům (zranitelnosti, malware kampaně, krádeže uživatelských údajů,…);
  - Publikování zpráv/aktualit (@GOVCERT_CZ).

Shrnutí prezentace

- Získali jste základní **informace** o NCKB/GovCERT.CZ;
- Poznali **roli** CERT týmu v kontextu **koordinace** a **spolupráce**.

Národní centrum
kybernetické
bezpečnosti

Děkuji za pozornost!

Otázky?

Národní centrum
kybernetické
bezpečnosti

Ondřej Šrámek

o.sramek@nbu.cz