VLÁDNÍ CERT (GovCERT.CZ)

Ing. Jakub Veselý
ředitel
odbor vládní CERT

Národní úřad
pro kybernetickou
a informační bezpečnost

GovCERT.CZ

- Kritická informační infrastruktura
- Významné informační systémy
- **Státní správa**
- Provozovatelé základních služeb
- Poskytovatelé digitálních služeb

- Proaktivní: sdílení informací, testování, vzdělávání, podpora
- Detekce: síťové anomálie, ochranné systémy, otevřené zdroje
- Reaktivní: zvládání incidentů, koordinace, analýzy

Spolupráce

- Mezinárodní skupiny
  - CSIRT network
  - TF-CSIRT
  - FIRST
- Evropská unie, ENISA
- NATO, CCD COE
- Policie ČR
- Bezpečnostní složky ČR
- Univerzity a vysoké školy

TF-CSIRT
Trusted Introducer

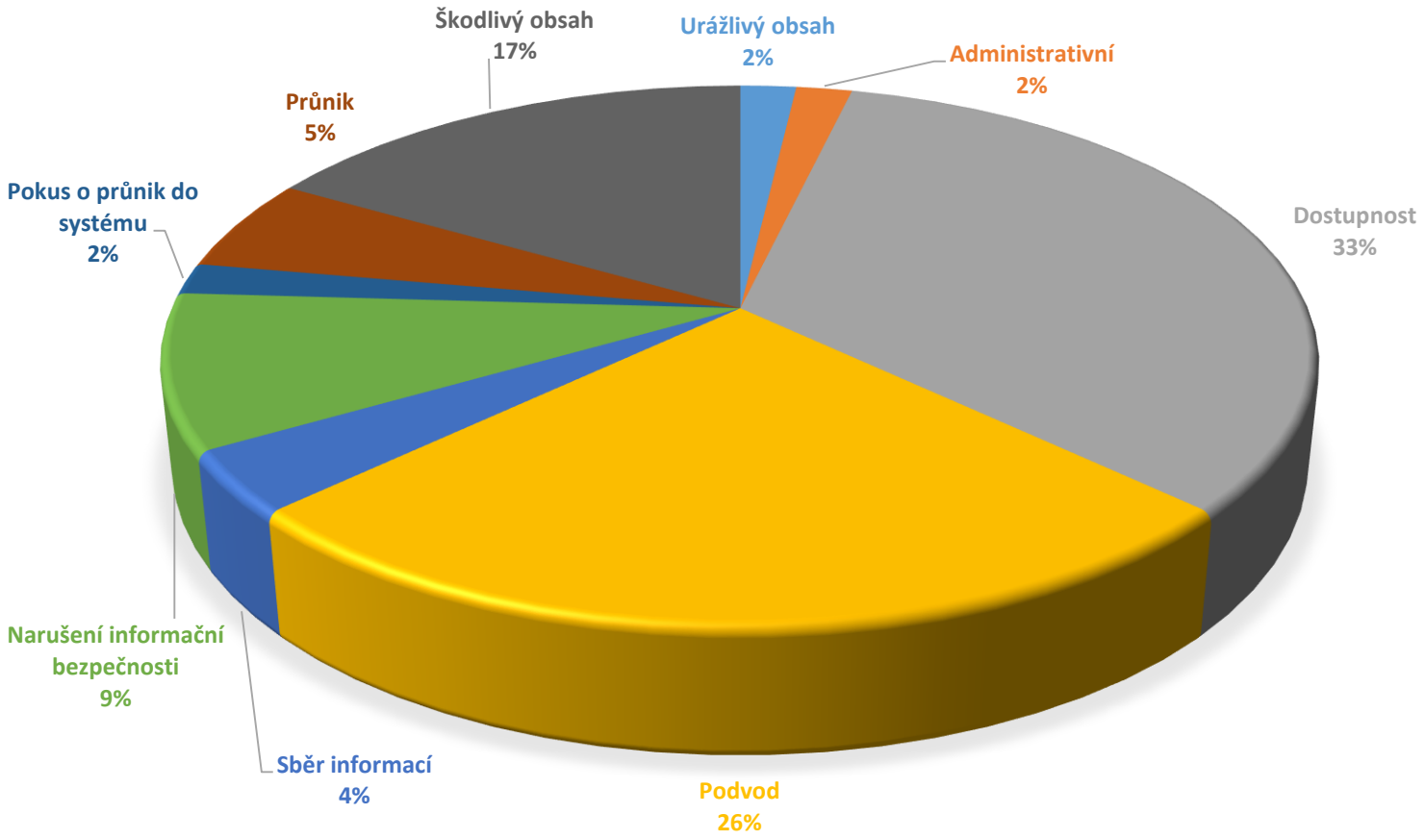
enisa
European Network and Information Security Agency

CCDCOE

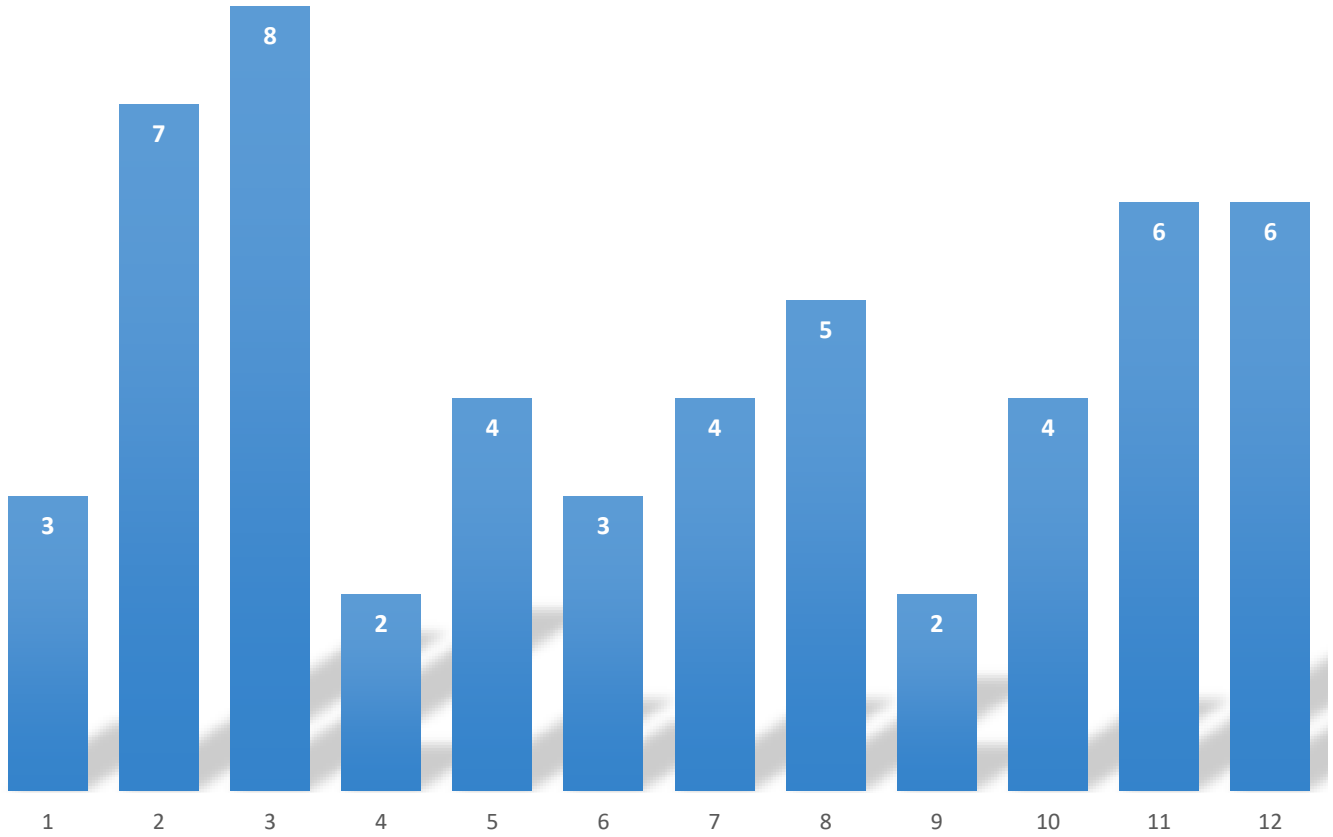
Oddělení reaktivní

- Zabezpečuje agendu řešící bezpečnostní incidenty
- Koordinuje kroky při jejich řešení a snaží se jim účinně předcházet
- Udržuje aktuální evidenci o všech řešených bezpečnostních incidentech
- Provádí sběr dat z veřejných a neveřejných zdrojů za účelem informování dotčených subjektů o zranitelnostech
- Provozuje SCADA laboratoř za účelem zabezpečení průmyslových systému

Klasifikace incidentů za rok 2018



Incidenty za rok 2018



Oddělení analýzy síťového provozu

- Analýza síťových artefaktů při řešení kybernetických incidentů
  - Logy z webových služeb, firewallů, obecně síťových prvků apod.
  - PCAP soubory, Flow záznamy
- Centrální analytický software GovCERT
- Projekt Honeypot
  - Cílem je nabízet virtuální image s honeypoty pro detekci pokusů útoků na služby v síti
  - Založeno na opensource nástrojích: cowrie, dionaea, snare tanner, conpot …
  - Prozatím ve fázi testování a příprav interně
  - Využití výstupů - napojení na GovCERT API pro obohacení dat ve Splunk (analytický SW)
- Školení síťové forenzní analýzy
  - Školení pro síťové analytiky
  - Seznámení s nástrojem Moloch a jeho možnostech při analýze většího množství PCAPů
  - Forenzní postupy pro zpracování síťových dat
- Projekt vybudování národního Scrubbing centra

Centrální analytický software GovCERT.CZ

- Založeno na platformě Splunk + Splunk Enterprise Security + doplňky
- Kolektory jsou připojeny přes IPsec tunely – autentizace obou stran
- Systém detekce globálních problémů nad Flow záznamy a událostmi ze sond
- Aktuálně zapojeno 7 státních institucí
- Probíhá vyhodnocování a distribuce blacklist IP, URL nebo domén pro Flowmon
- Detekční pravidla „BPATTERNS“ – signatury chování nad flow
- Koncem roku je v plánu zapojeních dalších institucí - Poslanecká sněmovna, Kancelář prezidenta republiky a MZe
- V dalším roce zapojení dalších 7 institucí

Oddělení analýzy síťového provozu

- Projekt Honeypot
  - Cílem je nabízet virtuální image s honeypoty pro detekci pokusů útoků na služby v síti
  - Frontend MHN (Modern Honey Network)
  - Založeno na opensource nástrojích: cowrie, dionaea, snare tanner, conpot …
  - Prozatím ve fázi testování a příprav interně
  - Využití výstupů - napojení na GovCERT API pro obohacení dat ve Splunk (analytický SW)
- Školení síťové forenzní analýzy
  - Školení pro síťové analytiky
  - Seznámení s nástrojem Moloch a jeho možnostech při analýze většího množství PCAPů
  - Forenzní postupy pro zpracování síťových dat
- Projekt vybudování národního Scrubbing centra

Oddělení analytické

- Forenzní analýza
  - Analýzou digitálních stop získaných v průběhu řešení kybernetických bezpečnostních incidentů
- Analýza malware
  - Získat IoC pro zamezení šíření
  - Popis schopností malwaru
- Forenzní analýza mobilních zařízení
- Spolupráce s PČR, BIS, VZ, UZSI při řešení závažných bezpečnostních incidentů na úrovni konzultantů

Aktuální trend malwaru

- Hlavní hrozbou stále ransomware
- Stále větší postup ke kryptominerům
- Větší sofistikace phishingu
  - Využívání databází s uniklými osobními údaji a hesly ke zvýšení důvěryhodnosti

Oddělení vývoje a bezpečnostního testování

- Hlavní agendou oddělení je vývoj, nasazení a zabezpečení aplikací jak pro vnitřní potřebu odboru Vládní CERT, tak i pro externí subjekty
- Příprava a koordinace kyberbezpečnostního cvičení Cyber Czech
- Projekt GovCERT API
  - Cíl sloučit zdroje různého informačního charakteru a tyto informace zpřístupnit přes jediné rozhraní
  - Informace z blacklistů, IoC databází, seznamů TOR koncových uzlů nebo informací o geolokaci zdroje
  - Implementováno s ohledem na zajištění vysoké dostupnosti
- Zajištění technické části kontrol povinných subjektů dle Zákona o kybernetické bezpečnosti

Oddělení vývoje a penetračního testování

- Poskytování interních a externích penetračních testů
  - Simulace útočníka
  - Proaktivní ochrana
  - Black-box - Grey-box
- Cílem je
  - Identifikovat zranitelnosti
  - Návrh pro posílení bezpečnosti

Mezinárodní cvičení

- LockedShields(CCDCOE)
  - 2014 –2. místo (v týmu společně s CERT.LV z Lotyšska)
  - 2015 – 7. místo
  - 2016 – 5. místo
  - 2017 – 1. místo
  - 2018 – 3. místo
  - **2019 – 2. místo**
- CyberCoalition(NATO)
- CyberEurope(ENISA)

Děkuji Vám za pozornost

Prostor pro dotazy

cert@nukib.cz

j.vesely@nukib.cz