GovCERT.CZ a řešení incidentů

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Národní úřad
pro kybernetickou
a informační bezpečnost

Ing. Jiří Valtr

Vedoucí oddělení Incident Handlingu, Vládní CERT

E-mail: jiri.valtr@nukib.gov.cz
Mobil: +420 601 694 830
PGP: F928 3DB4 4341 34CF C875 5F14 53FA 9CE5 97DE C37C

Jakub Onderka

Product Owner Portálu NÚKIB, DevSecOps
E-mail: jakub.onderka@nukib.gov.cz

Jak vládní CERT řeší incidenty ?

Co hlásit?

Do kdy hlásit?

Jak to hlásit?

Co ostatní nařízení?

GovCERT.cz

- Computer Emergenecy Response Team
- ~ cca 35 zaměstnanců
- 3 oddělení (a tři suboddělení)
  - (IH, OAKI, OPT)

"Government CERT (GovCERT.CZ) and CSIRT-type teams play a key role in protecting critical information infrastructure and important information systems according to the Cyber Security Act (181/2014 Coll.) and its implementing regulations."

GOVCERT.CZ

Po iniciačním hlášení

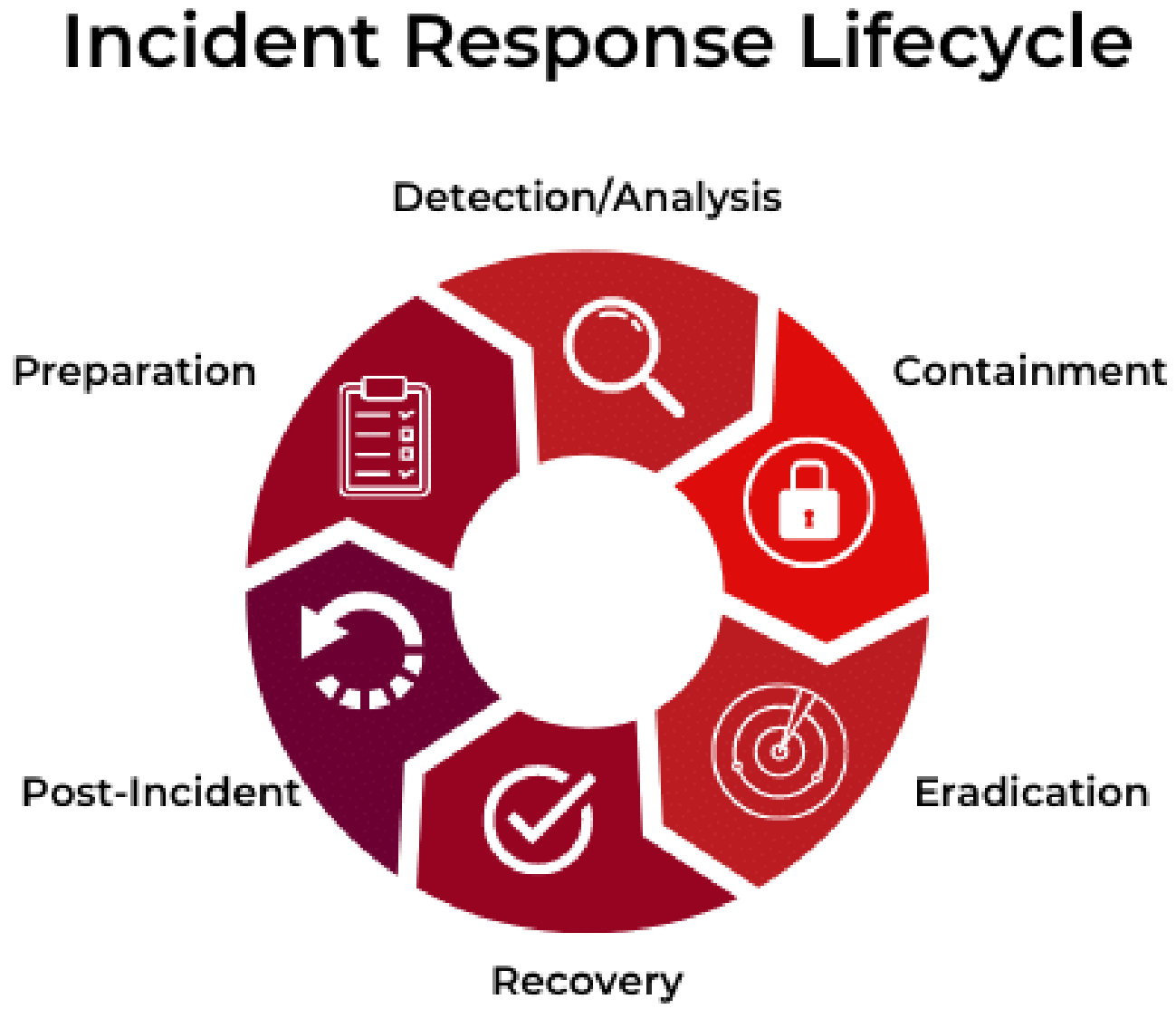
- Vyžádání relevantních dat
- Zjišťování informací (strategické / technické)
- Sladění očekávání
- Poskytnutí, co zrovna víme
- Nabídnutí metodické a analytické pomoci

Metodická podpora

Časté chyby:

- Zanedbaná identifikace
- Přeskočený containment
- Uspěchaná eradikace nebo eradikace za pochodu
- Nepřenesení lessons-learned do preparace

- Špatný OpSec (media, VT, …)



Forenzní analýza

- Mostly analysis of hard drives and RAM
- Tools:
  - Magnet Axiom
  - Encase
  - Autopsy
  - Tools from linux distro SIFT, CAINE
  - TimeScatch
  - Volatility
  - Redline
- Online tools:
  - VirusTotal
- Analysis output is usually set of IoCs, TTPs, malware for further analys

Malware analýza

- Analsis
  - Static
  - Dynamic
  - Automatic sandboxes
- Tools:
  - IDA Pro
  - Tools from linux distro REMnux and Windows Flare
  - Cuckoo, Joe Sandbox, HybridAnalysis, Tria.ge, VirusTotal
- Online nástroje
  - VirusTotal
- Analysis output is usually set of details about malware and his killchain. Usually described by TTPs. Also set of IoCs.

Síťová analýza

- Mostly analysis of logs from network devices, IDS/IPS, SIEM, firewall
- Tools:
  - Linux-bash
  - Wireshark, Tshark
  - NetworkMiner
  - Zeek, Suricata, Moloch (Arkime)
  - ElasticSearch + Logstash
  - Splunk
  - GeoIP + ASN
  - PassiveDNS
  - VirusTotal
- Analysis output is usually set of IoCs, TTPs, malware…

Threat hunt podpora

- Vytěžování těch dohledových nástrojů, které už máte nasazené
- Nasazení velociraptora
- Nasazení síťové sondy

CTI analýza

Type	Audience	Description
Tactical CTI	SecOps Network deffenders Incident handling	Technical identificators
Operational CTI	Incident handling Threat hunting Security leadership	Technical identifiers enriched with contextual data
Strategic CTI	Security leadership Top management	Putting it all together

Národní úřad
pro kybernetickou
a informační bezpečnost

Kooperace a infosharing

Národní úroveň

- CSIRT.cz
- PČR/NCTEKK
- Tajné služby
- ISAC komunity

- Soukromý sektor

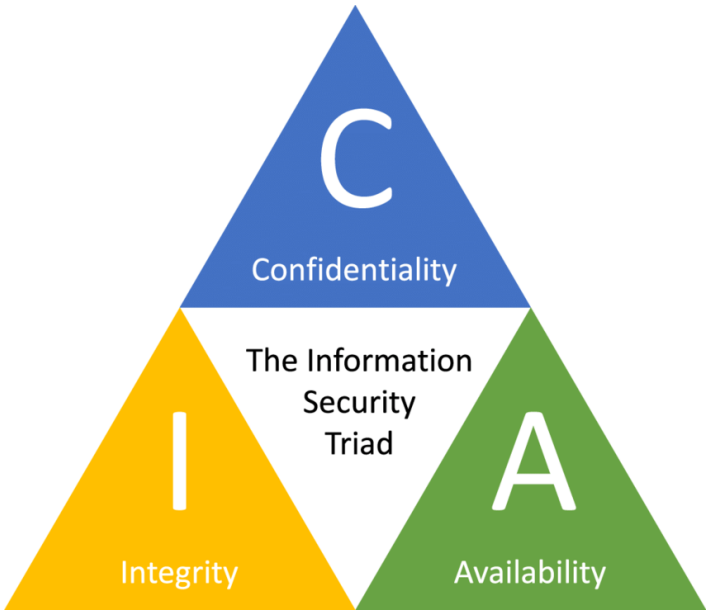
Mezinárodní úroveň

- CSIRTs Network
- TF-CSIRT
- FIRST
- Bilateral cooperation

Co hlásit?

Podle CIA

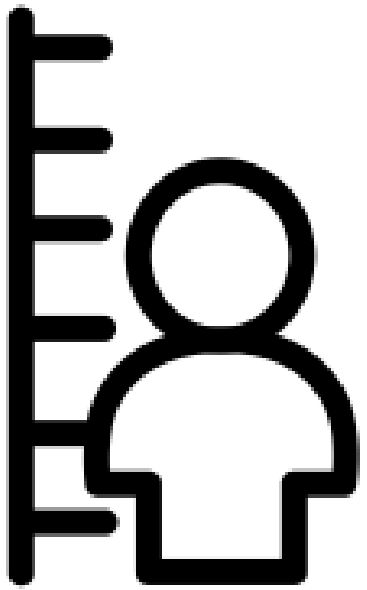
- Incidenty povinně
  - Došlo k narušení jednoho z prvků CIA
  - U Vás, nikoliv u Vašich zákazníků
- Události dobrovolně
  - Mohlo dojít k narušení CIA, ale nedošlo
  - Např. nepovedený, ale zajímavý bruteforce, nebo sken kritické 0-day
  - Pozor na opakující se události



Podle režimu

- Nižší
  - Hlásí pouze významné incidenty
  - Významnost si určují sami podle **§ 14 vyhlášky č. 410/2025 Sb.**
  - Podporu poskytuje primárně národní CSIRT tým.

- Vyšší
  - Hlásí všechny incidenty
  - O významnosti incidentu rozhodne CERT
    - U významných se pokračuje v ohlašovací povinnosti
    - U nevýznamných nejste povinni nic dohlašovat
  - Podporu primárně poskytuje vládní CERT tým



Do kdy hlásit?

Do kdy hlásit?

- Iniciační hlášení do 24h od zjištění incidentu

- **Oznámení** do 72 hodin od zjištění incidentu (kromě TSP)
- **Průběžnou zprávu** do 30 dní od **oznámení**
- **Závěrečnou zprávu** po uzavření incidentu

A co překopnutý kabel?

Dle nového zákona nemusíte hlásit incidenty:

- Kde není původ v kyberprostoru
- Lze vyloučit úmyslné zavinění

Nicméně v dle metodik doporučujeme hlásit, bude-li výpadek opakovaný

Jak hlásit?

Formulářem přes Portál

- Po obdržení rozhodnutí o registraci je možné incidenty hlásit pouze přes Portál NÚKIB
  - přes e-mail je možné hlásit incidenty pouze v případě nelze-li použít Portál (nedostupnost)
- **Incidenty může hlásit pouze statutární orgán nebo jím pověřený zástupce v Portálu**
  - Do budoucna zvažujeme zavedení pověření pouze pro oblast incidentů
- Vyšší i nižší režim hlásí jednotně přes Portál **do 24 hodin od zjištění**

- Přechodná lhůta jednoho roku:
  - Organizace regulované původním zákonem můžou hlásit incidenty podle původního zákona
  - Nově regulované organizace musí hlásit incidenty až po roce, do té doby dobrovolně a nemůžou požít hlášení podle původního zákona
- Je možné hlásit i incidenty nebo události dobrovolně
- Formuláře rovnou umožní přiložit např. vzorek malware nebo škodlivého e-mailu

Portál NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

PORTÁL NÚKIB | Chci vyřídit | Zákon o kybernetické bezpečnosti | NIS2 | Informační servis

Hlášení kybernetického bezpečnostního incidentu

Tato stránka slouží k **podání hlášení kybernetického bezpečnostního incidentu a k plnění oznamovací povinnosti** podle zákona č. 264/2025 Sb., o kybernetické bezpečnosti.

Volba právní úpravy pro hlášení incidentu

Volba právní úpravy pro hlášení incidentu: Subjekty, které byly regulovány podle starého zákona, mohou po dobu jednoho roku po účinnosti nového zákona podávat hlášení podle starého zákona, v souladu s přechodnou dobou stanovenou zákonem. Na tato hlášení se nebudou vztahovat lhůty stanovené novým zákonem. Nově regulované osoby: Osoby, které se staly regulovanými až podle nového zákona, musí podávat hlášení výhradně podle pravidel nového zákona.

Hlášení podle starého zákona

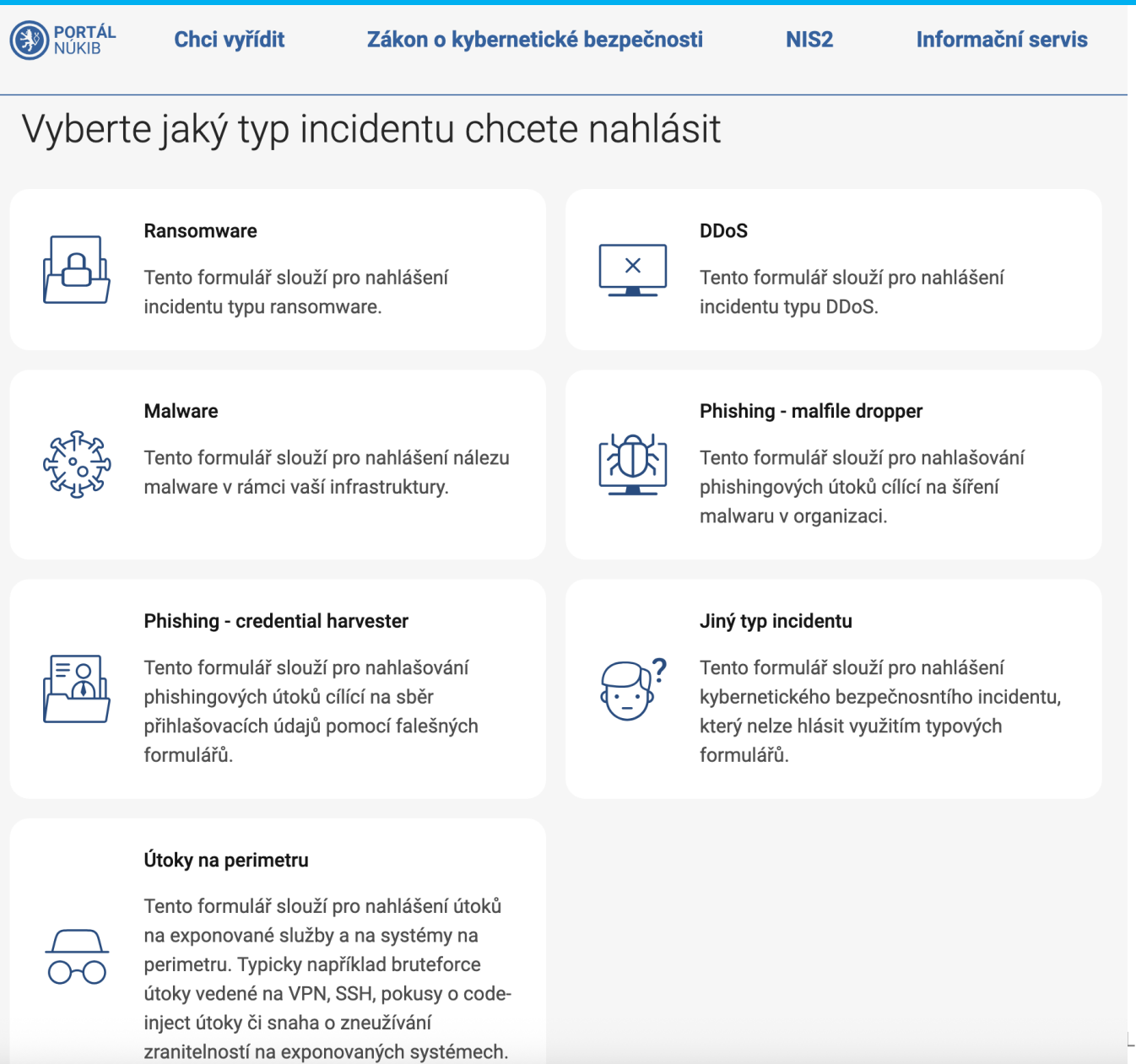
Hlášení kybernetického bezpečnostního incidentu podle starého zákona č. 181/2014 Sb.

Hlášení podle nového zákona

Hlášení kybernetického bezpečnostního incidentu podle nového zákona č. 264/2025 Sb.

Portál NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost



Bude možné hlásit incidenty přes API?

- V současné době ne
  - Formuláře se ještě budou vyvíjet na základě reálných zkušeností a zpětné vazby
  - Právní jistota hlášení
  - Vyplatí se vůbec?
- Zatím neexistuje zkušenost, kolik incidentů budou muset jednotlivé organizace hlásit
- Pokud organizace bude hlásit jednotky incidentů ročně, zavedení API se organizacím nevyplatí a naše úsilí nebude mít význam
- Vyhodnocení situace přibližně po roce

Národní úřad
pro kybernetickou
a informační bezpečnost

Děkujeme za pozornost

Dotazy?