

# GovCERT a řešení incidentů

NÚKIB



Národní úřad  
pro kybernetickou  
a informační  
bezpečnost



# Ing. Jiří Valtr

Reaktivní oddělení, Vládní CERT

E-mail: [jiri.valtr@nukib.gov.cz](mailto:jiri.valtr@nukib.gov.cz)

Mobil: +420 601 694 830

PGP: F928 3DB4 4341 34CF C875 5F14 53FA 9CE5 97DE C37C



# Jak vládní CERT řeší incidenty ?

## Co hlásit?

## Jak to hlásit?

## Co ostatní nařízení?



- Computer Emergency Response Team
- ~ 40 – 50 zaměstnanců
- 6 oddělení (a tři suboddělení)
  - (RO, OA, OASP, SecOps, OPT, OBOT)

*"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**



- Vyžádání relevantních dat
- Zjišťování informací (strategické / technické)
- Sladění očekávání
- Poskytnutí, co zrovna máme, atd...

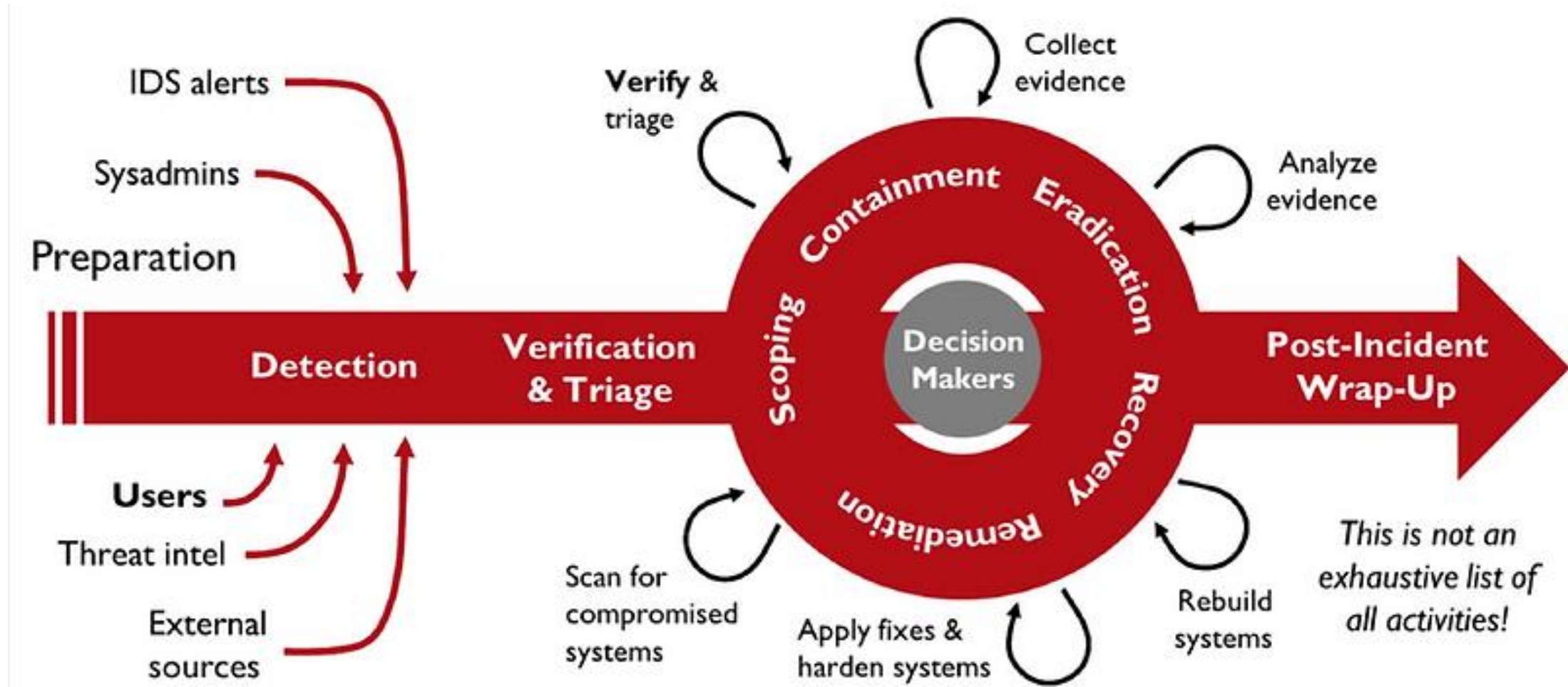


## Incident Response Lifecycle



### Časté chyby:

- Zanedbaná identifikace
- Přeskočený containment
- Uspěchaná eradikace nebo eradikace za pochodu
- Nepřenesení lessons-learned do preparace
- Špatný OpSec (media, VT, ...)





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





- 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 analysis





- 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.





- 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...





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



# Kooperace a infosharing



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

**CZ.nic**





- CSIRTs Network
- [TF-CSIRT](#)
- [FIRST](#)
- Bilateral cooperation





# Co hlásit?

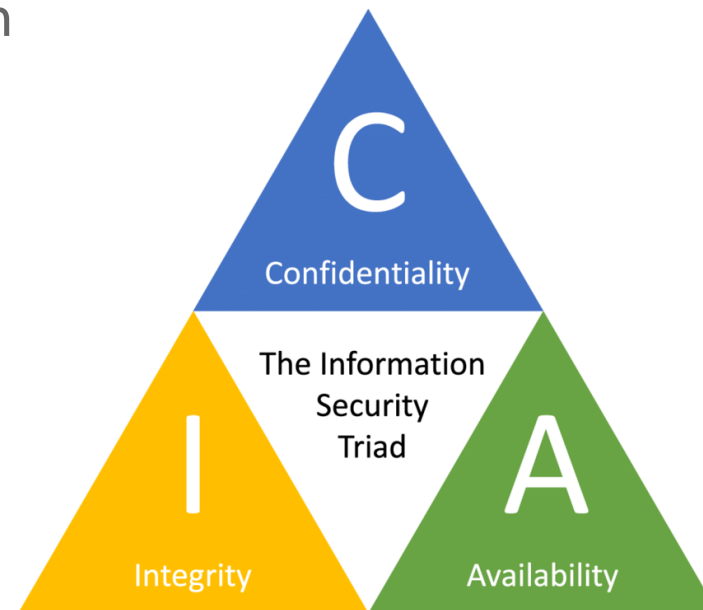


- Incidenty povinně

- Došlo k narušení jednoho z prvků CIA
- U Vás, nikoliv u Vašich zákazníkům

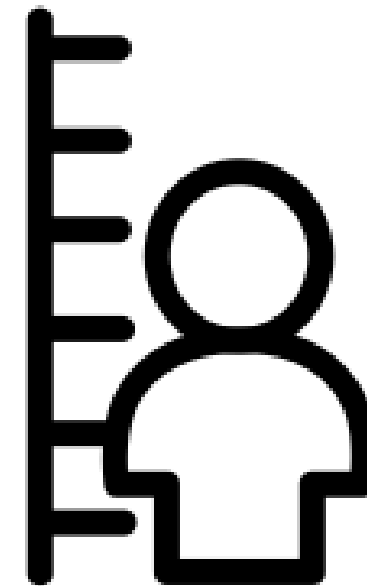
- Události dobrovolně

- Mohlo dojít k narušení CIA, ale nedošlo
- Např. nepovedený ale zajímavý bruteforce





- Nižší
  - Hlásí pouze významné incidenty
  - Významnost si určují sami
  - 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





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?



Typové formuláře budou dostupné zprvu pro:

- Ransomware
- DDoS
- Nález Malware
- Phishing – credential harvester
- Phishing – malware dropper
- Útoky na perimetru
- Jiné

Záložní možnost je e-mailem na [cert@nukib.gov.cz](mailto:cert@nukib.gov.cz)



- <https://portal.nukib.gov.cz/>
- Nejprve je však třeba registrovat službu
- Formulář ohlášení regulované služby bude zveřejněn s účinností zákona (1. listopadu) na Portálu NÚKIB v sekci Chci vyřídit.
- Formulář může vyplnit statutární orgán organizace, případně pověřený zástupce (ten se pověřuje skrz další formulář na Portálu), kterého pověří statutární orgán.



- Staří konstituenti
  - Zatím dle starého ZKB
  - Až obdrží potvrzení o registraci, můžou (ale nemusí) dle nZKB (§71)
  - Až pomine rok od nabytí účinnosti zákona, tak musí dle nZKB.
- Noví konstituenti
  - Až obdrží potvrzení o registraci, hlásí dle nZKB.



The screenshot displays the NUKIB portal interface. At the top, there is a navigation bar with the NUKIB logo and menu items: 'Chci vyřídit', 'Zákon o kybernetické bezpečnosti', 'NIS2', 'Informační servis', and 'EN'. A 'Odhlásit se' button is also present. Below the navigation bar, a 'Přehledový panel' (Dashboard) is visible, showing the user's name 'Marek Mészner'. The main content area is titled 'Chci vyřídit' and 'Správa regulovaných služeb' (Management of regulated services). It features several interactive cards:

- Ohlášení regulované služby**: Ohlášení splnění podmínek pro registraci podle § 6 zákona o kybernetické bezpečnosti.
- Hlášení údajů k regulované službě**: Hlášení kontaktních a doplňujících údajů podle § 11 zákona o kybernetické bezpečnosti.
- Žádost o zrušení registrace regulované služby**: Žádost o zrušení registrace podle § 10 zákona o kybernetické bezpečnosti.
- Přehled ohlášených služeb**: Zobrazení přehledu dosud nahlášených regulovaných služeb u dané organizace.
- Hlášení incidentu** (Section):
  - Hlášení incidentu dle původního zákona**: Hlášení kybernetického bezpečnostního incidentu podle původního zákona č. 181/2014 Sb.
  - Hlášení incidentu**: Hlášení kybernetického bezpečnostního incidentu podle § 15 zákona o kybernetické bezpečnosti.
- Správa zástupců** (Section):
  - Pověření/odstranění zástupce přes Portál NUKIB**: Statutární orgán organizace může pověřit nebo odvolat zástupce, který provádí veškeré další úkony.
  - Pověření zástupce datovou schránkou**: Tuto možnost lze použít pouze v případě zahraničních statutárů nebo zástupců bez českých dokladů totožnosti.
  - Odstranění zástupce datovou schránkou**: Tuto možnost lze použít pouze v případě zahraničních statutárů nebo zástupců bez českých dokladů totožnosti.

A 'Nahlásit chybu' button is located in the bottom right corner of the main content area.



# Co další regule?



- Subjekty spadající pod DORA hlásí incidenty ČNB skrze formulář ČNB
- ČNB však neposkytuje žádnou kyberbezpečnostní podporu.



- Stejný způsob hlášení / rozdílné podmínky hlášení
- Všechny hlášené incidenty jsou automaticky významné
- TSP mají kratší lhůtu pro oznámení
  - 24 hodin namísto 72 hodin od zjištění incidentu



# Děkuji za pozornost

## Dotazy?