



Kybernetické bezpečnostné incidenty a ich riešenie

Ján Doboš

Národné centrum kybernetickej bezpečnosti SK-CERT

Národný bezpečnostný úrad



I. ČO CHRÁNIME?



Dáta sú ukladané, spracovávané, vyhodnocované, vizualizované, ...
... Hardware, software, informačné systémy, procesy



NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

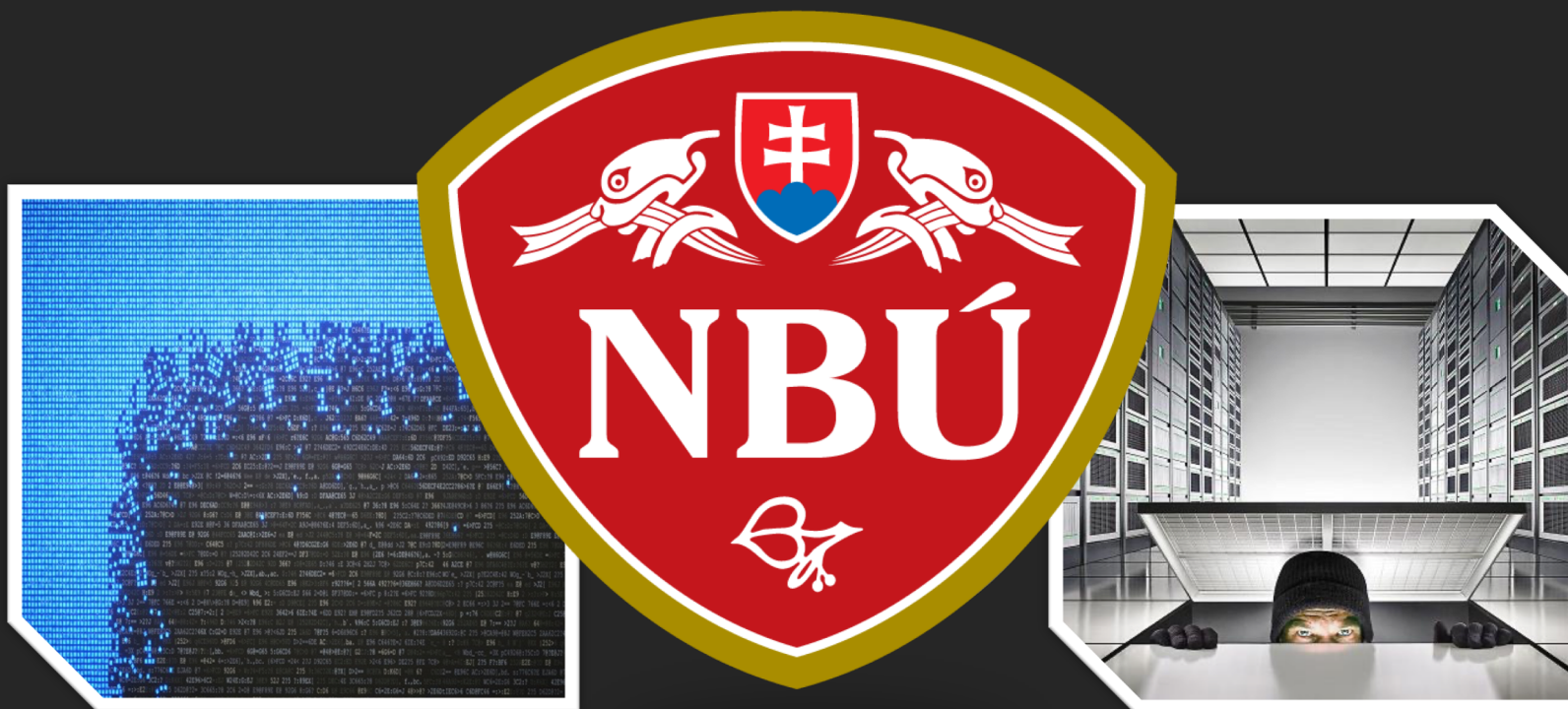
I. KTO NÁS OHROZUJE?



Script-kiddies, Hacktivists, ...
... Cybercriminals, APT



NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD



Zabezpečenia kybernetickej bezpečnosti IKT systémov a dát
Potreba vyhodnocovania obsahu informácií



NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

I. KYBERNETICKÝ BEZPEČNOSTNÝ INCIDENT



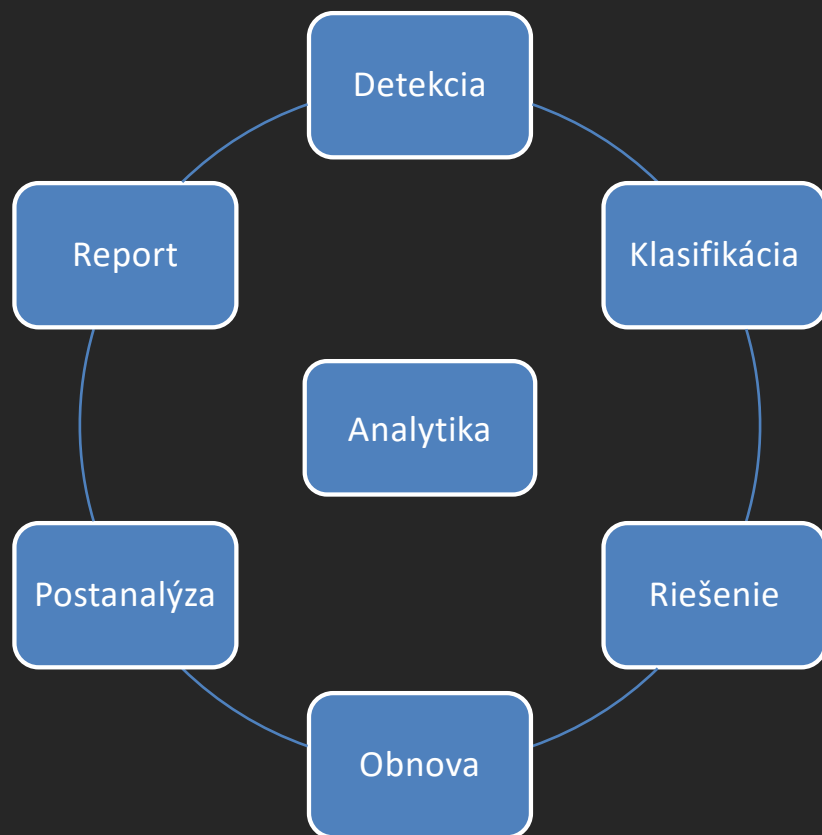
Akákoľvek udalosť s negatívnym vplyvom na kybernetickú bezpečnosť...
... Porušenie triády CIA, bezpečnostnej politiky alebo záväznej metodiky

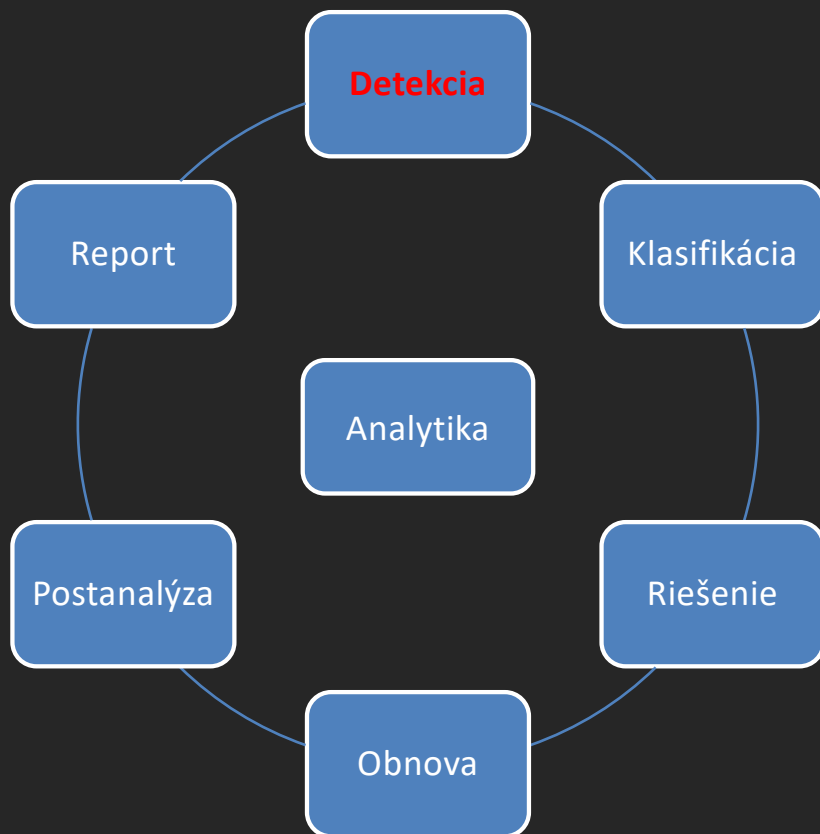


NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

- Zjednodušene:
 - Proces, ako incident vyriešiť a obnoviť pôvodný stav
- Detailný pohľad:
 - Určiť typ a závažnosť
 - Zastaviť prebiehajúci útok
 - Obnoviť stav a funkcionality pred útokom
 - Identifikovať útočný vektor a útočníka
 - Implementovať protiopatrenia

II. INCIDENT HANDLING – DEKOMPOZÍCIA NA FÁZY





- Ako sa o incidente dozvieme?
 - Štandardné komunikačné kanály
 - Špecializované technické prostriedky
 - Vlastná analytická činnosť

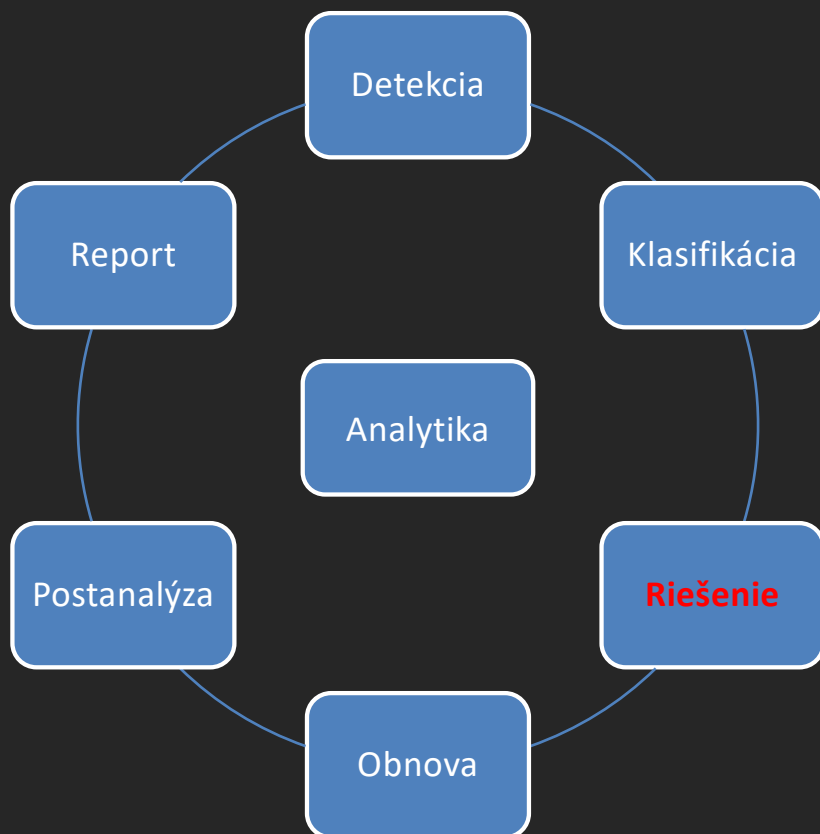
- Interné subjekty
- Externé subjekty

II. INCIDENT HANDLING – KLASIFIKÁCIA

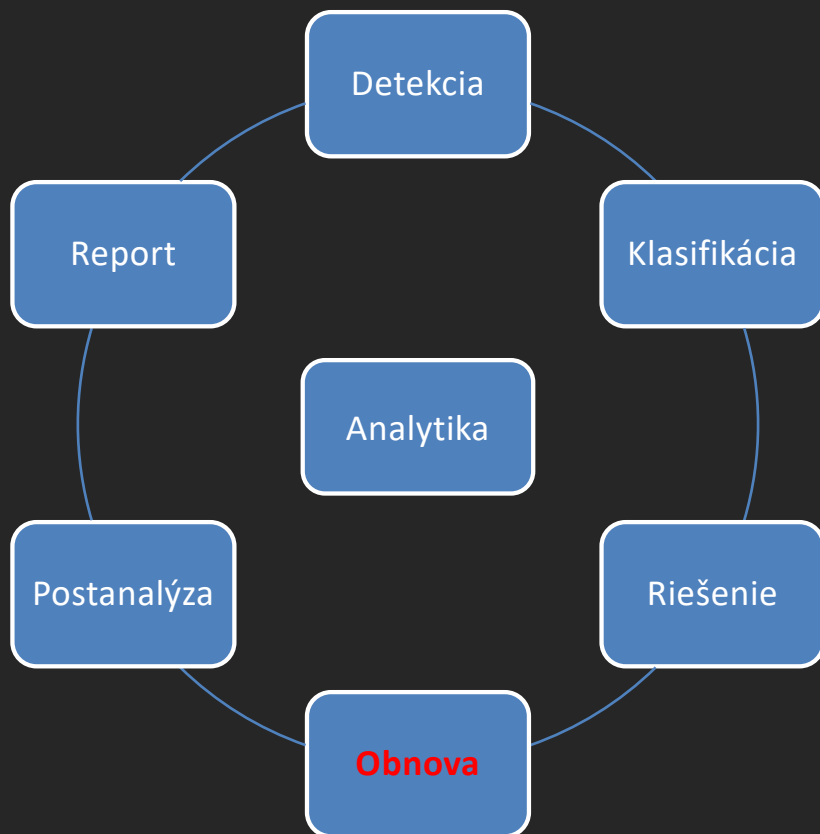


- Aké sú základné informácie o incidente?

- Udalosť vs. incident
- Má dopady na kybernetický priestor SR?
- Spadá riešenie incidentu pod nás?
- Technický typ incidentu
- Kategorizácia podľa zákona
- Eskalačné procesy
- Získať doplňujúce informácie
 - Rozsah škôd a dopady
 - Vzorky správ a malwaru



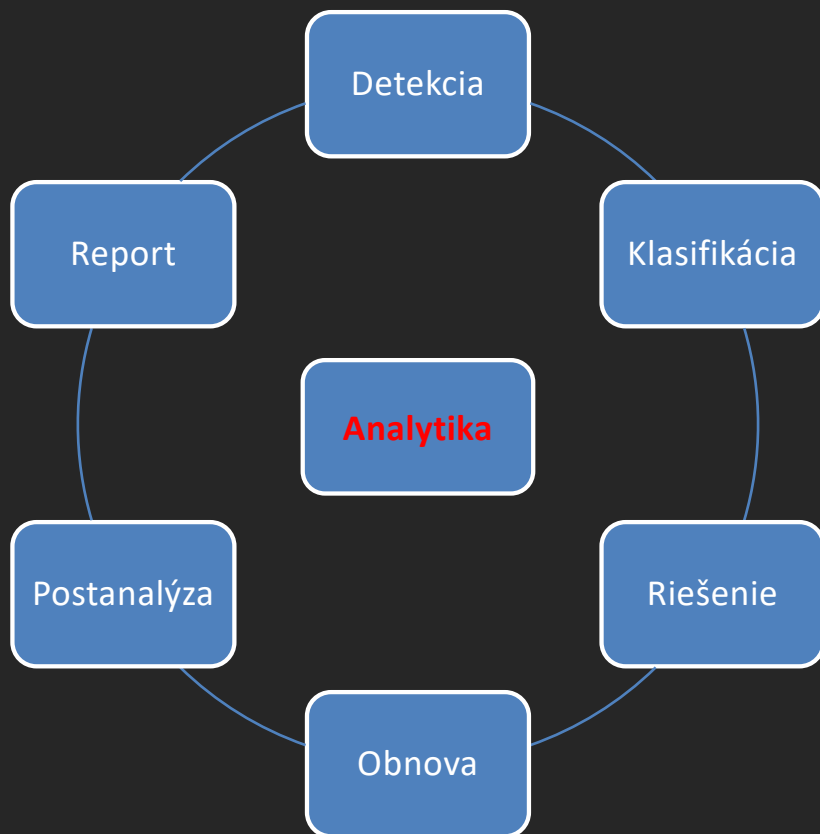
- Čo je potrebné urýchlene vykonať?
 - Zastaviť prebiehajúci útok
 - Odrezať útočníka, izolovať infikované zariadenia, odstrániť phishingový obsah, ...
 - ABUSE proces a odstránenie podozrivého/phishingového/škodlivého obsahu
 - Zaistiť dôkazy, logy a digitálny materiál pre ďalšiu analýzu
 - Nesprávna analýza môže znehodnotiť dôkazy



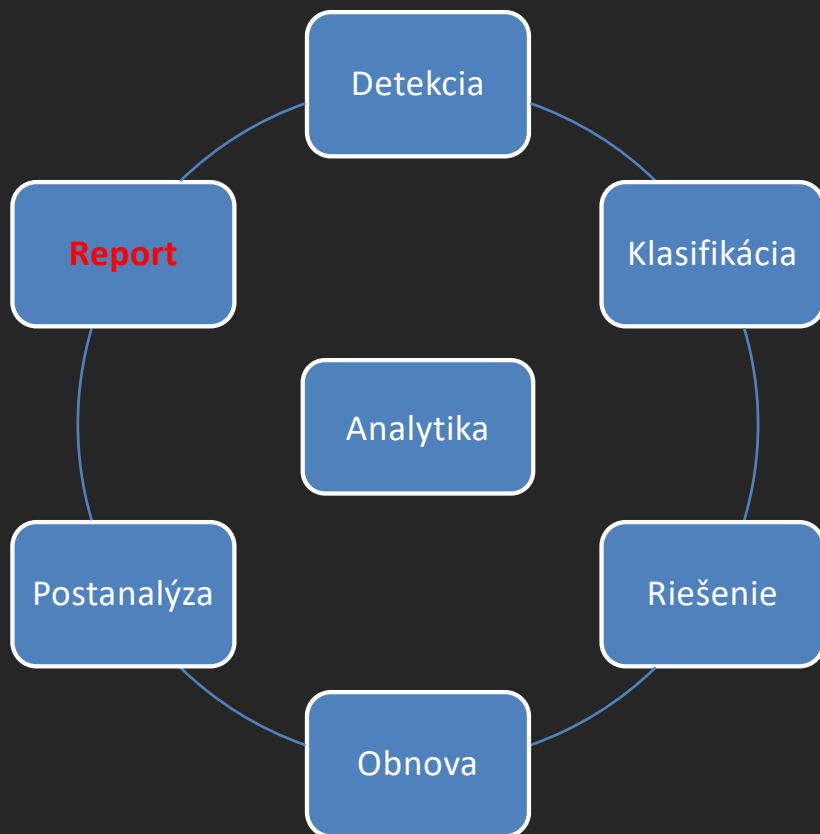
- Ako zaistíme obnovu do pôvodného stavu?
 - Obnova zo zálohy, reinštalácia zariadení, výmena poškodených komponentov, rozšifrovanie dát, ...
- Ako zabránime zopakovaniu incidentu?
 - Zmena prihlasovacích údajov a kryptografického materiálu
 - Hardening systému
 - Nasadenie dodatočných protopatrení
 - Procesy, metodiky



- Postupovali sme správne a efektívne?
 - Čo sme mohli spraviť lepšie a efektívnejšie?
 - Ako zabezpečiť, aby sa podobný incident nezopakoval?
 - Čo nemáme? Čo je potrebné zaviesť? Čo je potrebné zohnať a zabezpečiť?



- Čo všetko sprevádza základné fázy?
 - Stanovenie útočného vektora, prvotného vektora prieniku, modusu operandi útočníka, atď.
 - Forenzná analýza
 - Malwarová analýza
 - Threat intelligence, obohacovanie a korelácia dát

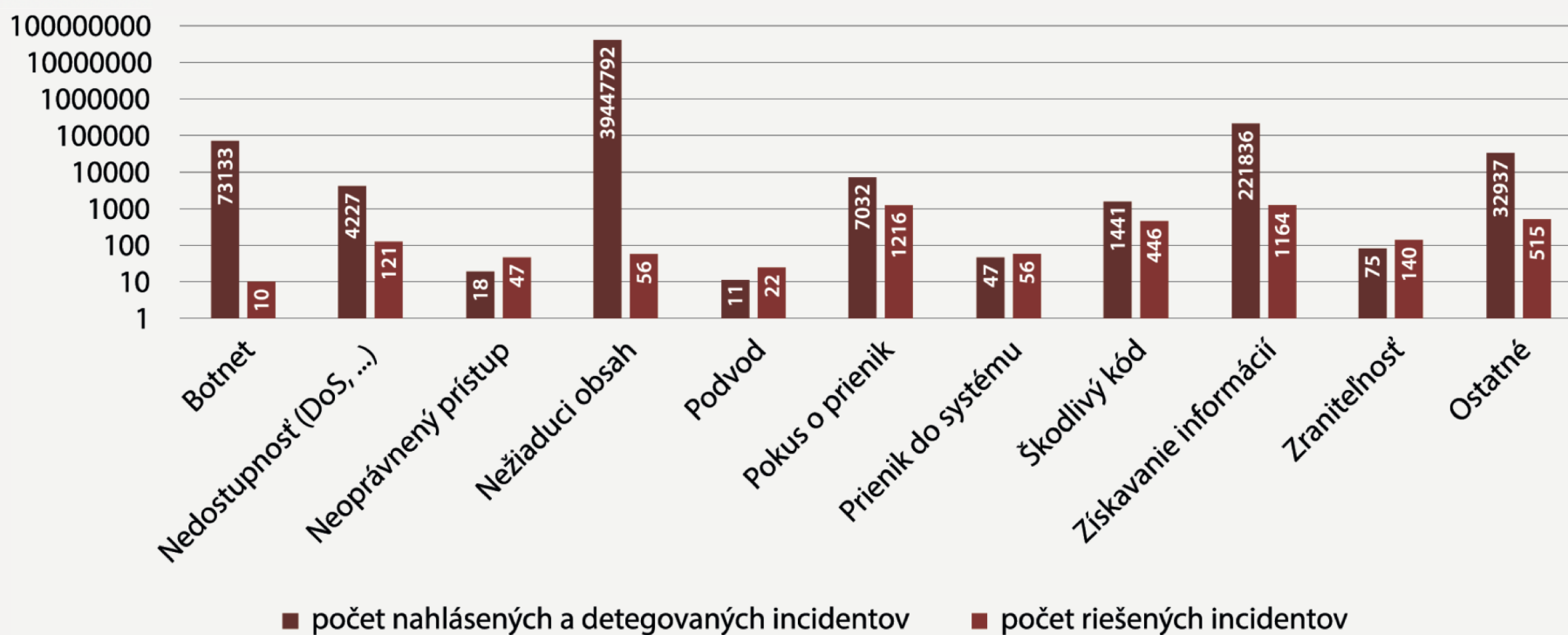


- Ako zistenia prezentovať?

- Základné informácie o subjekte
- Manažérske zhrnutie incidentu
- Časová os riešenia incidentu
- Analytické zistenia
- Odporúčania
- Zoznam indikátorov kompromitácie (IOC)

III. KYBERNETICKÝ PRIESTOR SR

Počet detegovaných, nahlásených a riešených incidentov v roku 2020. (Zdroj: NCKB SK-CERT).



- Najpočetnejšie typy incidentov:
 - Nežiadúci obsah a získavanie informácií
 - Skenovanie a pokusy o prienik
 - Malware
 - Zraniteľnosti a nesprávna konfigurácia zariadení a systémov



- Útok kombinujúci technické vedomosti s princípmi sociálneho inžinierstva
- Primárne ciele
 - Získavanie citlivých údajov
 - Šírenie rôznych foriem malwaru
- Sekundárne ciele
 - Zneužitie získaných údajov a infikovaných zariadení na škodlivú činnosť
 - Obchodovanie

Všetci sme o nich počuli, napriek tomu je obetí stále veľa...



IV. ŠPECIFICKÉ TYPY PHISHINGOVÝCH E-MAILOV V SR

- Možno legitímne

- SPAM

- Vydieranie a vyhrážanie

Sextortion

- Prvotný kontakt a získavanie údajov

Higher management impersonation

- Dezinformácie

- Šírenie phishingových URL

Malwaretisement

Špecifické typy incidentov vyžadujú špecifický prístup k IH



IV. VŠEOBECNÉ FÁZY PHISHINGOVÉHO ÚTOKU

- Voľba cieľa
- Analýza cieľa
- Tvorba a umiestnenie obsahu
- Infekcia a obeť
- Zber a exfiltrácia dát
- Detekcia, nahlásenie a odstránenie obsahu
 - ABUSE proces a jeho problémy

IV. AKO ROZPOZNAŤ PHISHINGOVÝ ÚTOK - KYBERHYGIENA



- Bud'te obozretní a prípade pochybností overte odosielateľa a obsah správy
- Používajte zložitejšie heslá
- Pravidelne aktualizujte používané programy
- Pravidelne zálohujte
- Používajte antivírus
- **Nesnažte sa opraviť problém a kontaktujte Vaše IT oddelenie alebo Národné centrum kybernetickej bezpečnosti SK-CERT**



NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

- Viacero prístupov k analýze principiálne spadajúcich do dvoch kategórií
- **Primitívna analýza (vizuálna inšpekcia a interakcia)**
 - Obeť, URL, SSL/TLS, responzívny dizajn, linkovanie, validácia vstupov
- **Hĺbková analýza (technická analýza a použitie špecializovaných nástrojov)**
 - HTTP komunikácia, presmerovania, snímky obrazovky, analýza zdrojového kódu
- **Dávajme si pozor!!!**
 - Mať prehľad o aktuálnych trendov
 - Kritickým komponentom naďalej zostáva zdravý rozum a analytické myslenie človeka
 - Čokoľvek podozrivé je potrebné overiť

- Definícia
 - Úmyselná alebo neúmyselná chyba HW, SW alebo P ktorú môže byť zneužitá a viesť k vzniku kybernetického bezpečnostného incidentu
- Faktory
 - Človek
 - Ekonomický tlak a tlak zákazníkov na vývojárov a výrobcov
 - Komplexnosť aktuálneho stavu IKT a kybernetického priestoru
 - Komplexné systémové architektúry a frameworky
 - Brotnobyte-y dát
 - Strojové učenie a umelá inteligencia
- Identifikácia a klasifikácia závažnosti (CVE, CVSS, počet zraniteľných zariadení)

- V kybernetickom priestore možno pozorovať narastajúci počet zraniteľností
- Zneužitie zraniteľnosti
 - Oblúbený útočný vektor
 - Možné závažné dopady na CIA triádu a ďalšie aspekty kybernetickej bezpečnosti
- Zverejnenie zraniteľnosti a jej odstránenie
 - Kritické pre udržanie kybernetickej bezpečnosti
 - Malo by sa riadiť pravidlami zodpovedného zverejňovania zraniteľností
 - Kontinuálny proces adaptácie na dynamicky sa meniaci ekosystém zraniteľností
 - Medzinárodná spolupráca a výmena informácií a procesov

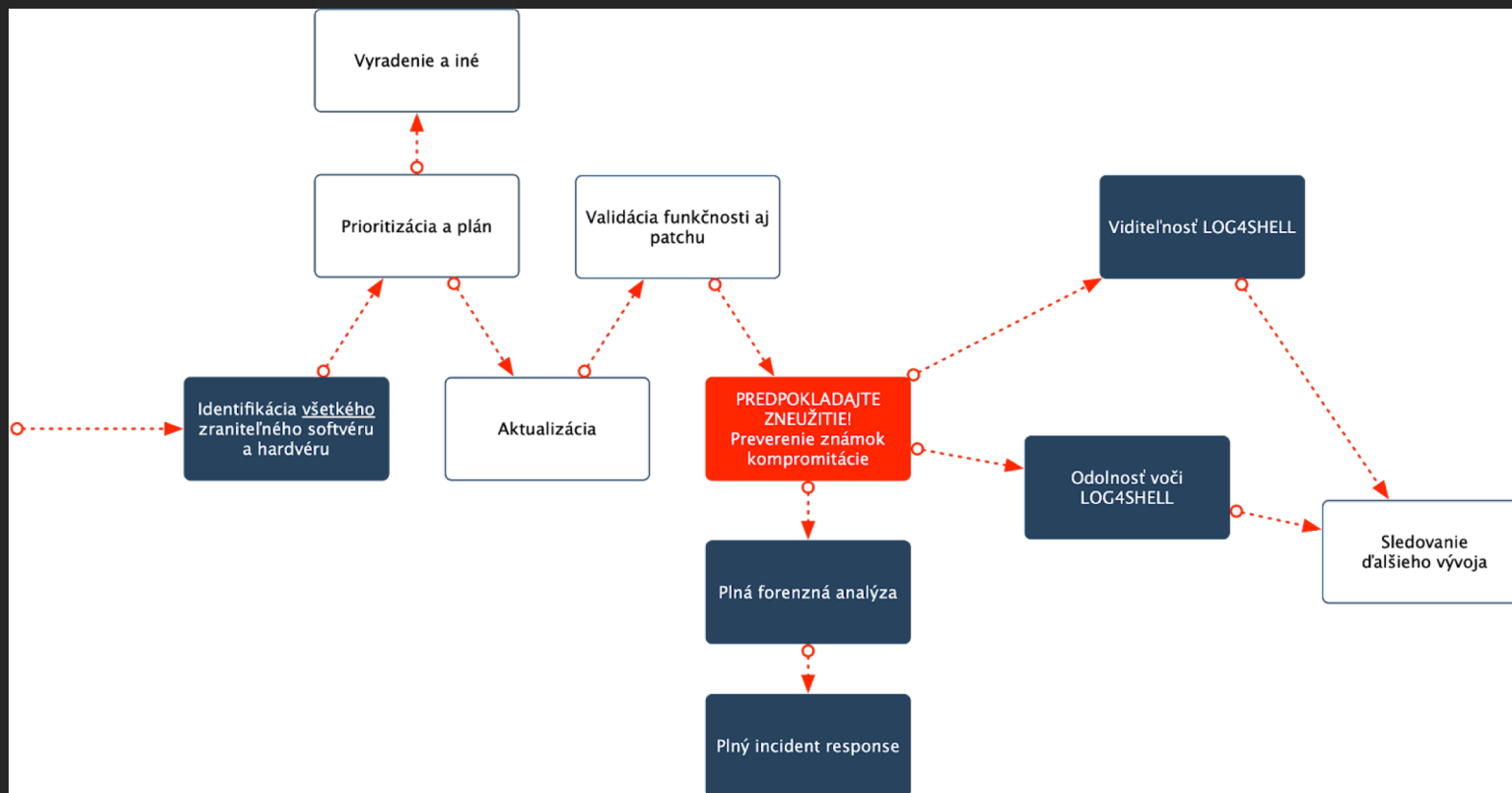
Nesprávna konfigurácia je problém sám o sebe.



Knižnica log4j od spoločnosti Apache, naprogramovaná v jazyku Java, pomáha aplikáciám ukladať záznamy o aktivite, tzv. logy. Keďže logovanie je dobrou praxou a knižnica log4j je jednou z najrozšírenejších na platforme Java, nachádza sa v širokom portfóliu aplikácií a služieb vrátane aplikácií popredných výrobcov.

Knižnica log4j je používaná **v rámci softvérových produktov aj fyzických zariadení, kde môže byť zneužitá bez akejkoľvek autentifikácie či znalosti prístupových údajov.**

- Analýza najväčšieho repozitára balíkov Java, Maven Central, ukázala že až 35.000 balíkov (viac než 8% z celkového počtu) obsahuje závislosť na Log4j 2.
- Bezpečnostná komunita doposiaľ identifikovala 978 zraniteľných komerčných produktov od 417 svetových výrobcov. Zasiiahnuté sú produkty Apache (Struts2, Solr, Druid, Flink) a produkty svetoznámych spoločností ako Apple, Atlassian, Amazon, Cloudflare, Cisco, Elastic, UniFi, Twitter, Steam, VMware a mnohých ďalších.
- V tomto čísle nie sú zahrnuté zraniteľné produkty malých výrobcov alebo produkty vyrobené na mieru zákazníčkovi.



- Triviálne incidenty a ich riešenie môžu byť v skutočnosti komplikované
- Pohotovú reakcia
- Analytické, často out-of-the-box myslenie analytika
- Návrh vlastných nástrojov, kreatívne myslenie
- Komunikácia a výmena informácií na národnej i medzinárodnej úrovni
- Tímová práca

KONTINUÁLNA POTREBA ZLEPŠOVAŤ SA



Ďakujem za pozornosť.

