Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

NCC-SK
SLOVAKIA CYBERSECURITY COORDINATION CENTRE

Monitorovanie, hlásenie a riadenie udalostí a kybernetických bezpečnostných incidentov

Pavol Dovičovič

20. máj 2025

DEFINÍCIA POJMU „UDALOSŤ“

- **Udalosť – IT všeobecne:**
  - Akýkoľvek pozorovateľný jav v systémoch a v sieťach - napr. prihlásenie/odhlásenie používateľa, spustenie aplikácie, aktivita sieťovej vrstvy, transakcia, správa a pod. [NIST Special Publication 800.61, 2012: 1-147]
- **Udalosť – riadenie IT služieb:**
  - Akákoľvek zmena stavu, ktorá má význam pre manažment služby alebo iných konfiguračných položiek [ITIL®4: Glossary of terms]



Spolufinancovaný Európskou úniou

ČO JE TO „BEZPEČNOSTNÝ INCIDENT“

Bezpečnostný incident všeobecne:

- škodlivá udalosť, v rámci ktorej:
  - nastala strata dôvernosti dát,
  - nastalo zničenie dát,
  - nastalo prelomenie integrity systému,
  - došlo ku obmedzeniu, alebo odmietnutiu dostupnosti služby.

Atribúty „CIA“

Inak tiež:

Atribúty podvodu

- nezvyklá, alebo neočakávaná aktivita,
- priestupok, alebo riziko priestupku proti bezpečnostnej politike,
- priestupok, alebo riziko priestupku proti akceptovateľnému použitiu politík,
- nesplnenie štandardných postupov,
- použitie informačných aktív iným, než stanoveným, alebo dobromyseľným spôsobom.

Spolufinancovaný Európskou úniou

POŽIADAVKY NA RIADENIE ZÁZNAMOV UDALOSTÍ (LOGOV)

Log Management

POŽIADAVKY NA ZAZNAMENÁVANIE UDALOSTÍ

§ 15 Bezpečnostné opatrenia pre oblasť podľa § 20 ods. 3 písm. k) ZoKB

(1)

- Zaznamenávanie udalostí a monitorovanie sietí a informačných systémov sa uskutočňuje implementáciou centrálneho nástroja na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov zabezpečujúceho dohľad nad sieťami a informačnými systémami zaznamenávaním prevádzky týchto sietí a informačných systémov, a to najmenej v rozsahu

  a) centrálnych sieťových prvkov a serverov,

  b) služieb prístupných do externých sietí a

  c) kritických interných serverov a služieb.



POŽIADAVKY NA ZAZNAMENÁVANIE UDALOSTÍ

§ 17 Bezpečnostné opatrenia podľa § 20 ods. 3 písm. m) zákona

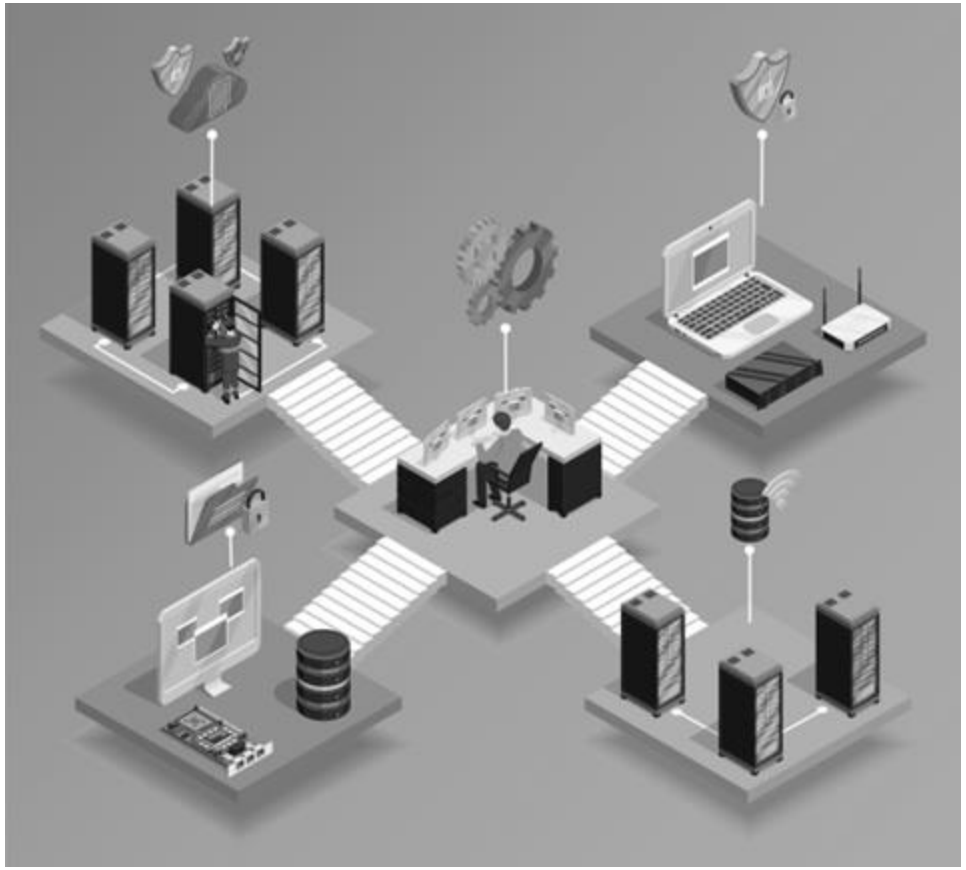
(1)

- Riešenie kybernetických bezpečnostných incidentov pozostáva najmä
  a) z prípravy a vypracovania štandardov a postupov riešenia kybernetických bezpečnostných incidentov,
  b) z monitorovania a analyzovania udalostí v sieťach a informačných systémoch,
  c) z detekcie kybernetických bezpečnostných incidentov,
  d) zo zberu relevantných informácií o kybernetických bezpečnostných incidentoch,
  e) z vyhodnocovania kybernetických bezpečnostných incidentov,
  f) z riešenia zistených kybernetických bezpečnostných incidentov a zníženia následkov zistených kybernetických bezpečnostných incidentov a
  g) z vyhodnocovania spôsobov riešenia kybernetických bezpečnostných incidentov po ich vyriešení a prijatia opatrení alebo zavedenia nových postupov s cieľom minimalizovať výskyt obdobných kybernetických bezpečnostných incidentov.

Spolufinancovaný Európskou úniou

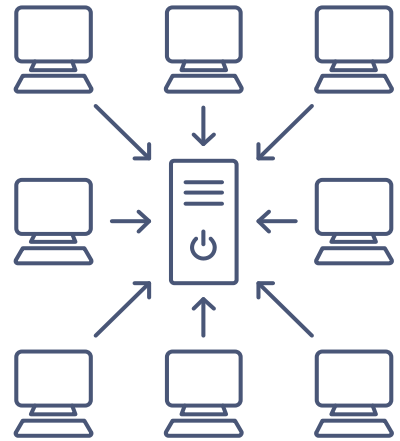
PREVÁDZKOVÝ MONITORING

- Účelom prevádzkového monitoringu je najmä nepretržité monitorovanie stavu a funkčnosti zariadení, vrátane non-IT infraštruktúry
- Predmetom prevádzkového monitoringu sú napríklad:
  - **fyzické vlastnosti prostredia** – bezpečnostné systémy, elektrické napájanie, teplota, vlhkosť vzduchu v dátovom centre, teplota komponentov, atď.
  - **stav IKT systémových ukazovateľov** – kapacita úložného priestoru, využitie operačnej pamäte, atď.
  - **logické stavy** – stav behu systému, alebo aplikácie, dostupnosť servera, alebo web stránky, exspirácia certifikátov atď.



BEZPEČNOSTNÝ MONITORING

- Aktivity používateľov v podobe **vytvorenia, čítania, aktualizácie** alebo **odstránenia** chránených a prísne chránených informácií a údajov, alebo ďalších informačných aktív s nimi spojených,
- **Iniciáciu pripojenia** a **akceptáciu alebo odmietnutie pripojenia so** zaznamenaním aspoň dátumu a času aktivity, identifikácie technického prostriedku, v rámci ktorého je činnosť zaznamenaná, identifikáciu osoby a zdroja vo forme IP adresy,
- **Pridelenie, úpravu** alebo **zrušenie prístupových práv** používateľa **vrátane pridania nového používateľa** alebo skupiny používateľov,
- **Zmenu úrovne oprávnenia** používateľa,
- **Zmenu pravidiel firewallu,**
- **Zmenu hesla,**
- Automatické **varovné alebo chybové hlásenia** systémov,
- Detegované **podozrivé alebo škodlivé aktivity,**
- Ďalšie **informácie nevyhnutné na posúdenie závažnosti** kybernetického bezpečnostného incidentu v spojení s kritickosťou danej služby alebo zariadenia a **korektné informácie o dátume, čase** a použitej časovej zóne.



TYPY ZÁZNAMOV - LOGOV

- Systémový log (System log)
- Bezpečnostný log (Security log)
- Aplikačný log (Application log)
- Log udalostí (Event log)
- Log o chybách (Error log)
- Log prístupov (Access log)
- Log transakcií (Transaction log)



ČO NELOGOVAŤ - PRÍKLADY

- Ktoré informácie **nie je vhodné** zapisovať do logov:
  - Heslá
  - Šifrovacie kľúče
  - Zdravotné informácie
  - Informácie o platobných kartách
  - Pozor na osobné údaje
- Ak potrebujete tieto údaje zaznamenať, tak je potrebné ich **anonymizovať.**
- Využitie:
  - Štatistiky
  - Detekcia prienikov
  - Ostatné



Riadenie incidentov

PROCES ODOZVY NA INCIDENT (INCIDENT RESPONSE)

Je proces:

- Preddefinovanej
- Formalizovanej
- Otestovanej

} **reakcie** na bezpečnostný incident



V aktivitách odozvy na incident by mali byť obsiahnuté dva základné ciele:

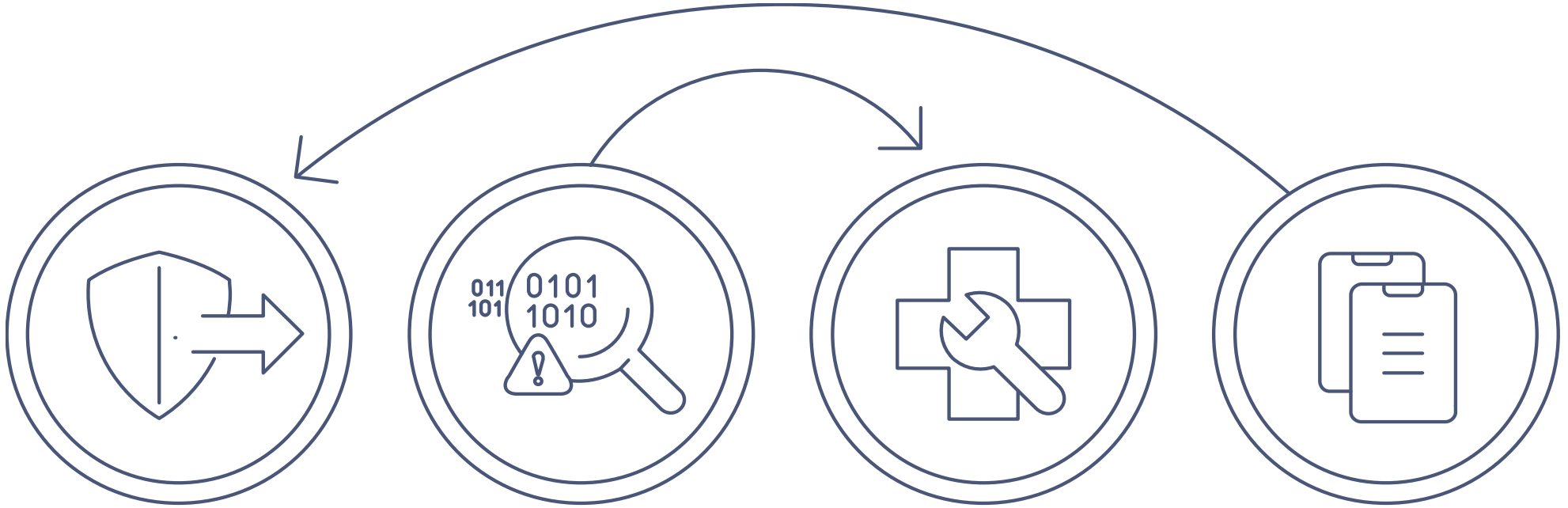
- **„Opraviť a pokračovať"**
  - Obnovenie funkčnosti poškodených informačných aktív a pokračovanie v činnosti.



- **„Vyšetriť a vyriešiť"**
  - Zákonná náprava a zhromaždenie digitálnych stôp na podporu postupu proti vinníkovi.



GENERICKÁ SCHÉMA PROCESU RIEŠENIA BEZPEČNOSTNÝCH INCIDENTOV



Plánovanie a testovanie → Detekcia a eskalácia → Analýza a kategorizácia → Vymedzenie a izolácia → Náprava následkov → Forenzná analýza → Post-incidentné aktivity

- *NIST Computer Security Incident Handling Guide*
- *ISO/IEC 27035:2011 Information technology -- Security techniques -- Information security incident management*

Spolufinancovaný Európskou úniou

PLÁN REAKCIE NA INCIDENT (CSIRP)

Plán reakcie na incident (CSIRP - Computer Security Incident Response Plan):

- Popis procesov súvisiacich so spôsobom riešenia bezpečnostného počítačového incidentu
- Diagnostická matica pre urýchlenie rozhodovania, resp. pre menej skúsený personál

Plán reakcie musí definovať minimálne nasledujúci rozsah procesov:

- Profilovanie systémov, určenie kritickosti procesov
- Definíciu „spúšťačov" (triggers), zdrojov indikácií a spôsobov notifikácie incidentov
- Komunikačná matica a popis hlavných postupov pre fázu reakcie na incident
- Podrobný popis spôsobu obsluhy incidentov, triedený podľa jednotlivých kategórií (optimálne - odkaz na bázu znalostí)
- Popis hlavných postincidentných aktivít
- Klasifikáciu hlásení, kategorizáciu a ohodnotenie závažnosti incidentov
- Spôsob, termíny a zodpovednosti za aktualizáciu a testovanie plánu
- Pripravenosť na použitie CSIRP v stresovej situácii (napr. checklist)



PRÍKLAD IRP (INCIDENT RESPONSE PLAN)

- **Identifikácia:**
  - Systémy monitorovania siete detegujú náhle zvýšenie sieťovej prevádzky (napr. HTTP GET požiadavky na web server).
  - Analyzujte logy a určite, či ide o DDoS útok (napr. veľký objem požiadaviek z rôznych IP adries).
- **Izolácia:**
  - Nasmerujte premávku cez firewall alebo DDoS mitigation systémy, aby sa filtrovali škodlivé požiadavky.
  - Aktivujte cloudové alebo CDN riešenia (ak sú dostupné) na rovnomerné rozloženie záťaže.
- **Eradikácia:**
  - Spolupracujte s poskytovateľom internetových služieb, aby pomohol blokovať škodlivé IP adresy.
  - V prípade pretrvávania útoku zvážte dočasné obmedzenie prístupu k službám z určitých geografických oblastí.
- **Obnova:**
  - Po skončení útoku obnovte normálnu sieťovú prevádzku a sledujte ďalšie podozrivé aktivity.
  - Uistite sa, že všetky služby sú opäť dostupné.
- **Post-incidentné kroky:**
  - Zdokumentujte rozsah útoku, jeho dopad a spôsob riešenia.
  - Aktualizujte plán mitigácie DDoS a implementujte ďalšie ochranné opatrenia, ako je napríklad lepšia CDN integrácia.

Spolufinancovaný Európskou úniou

SPÔSOBY TESTOVANIA IRP

- **Tabletop:**
  - Diskusné cvičenia, simulujúce rôzne scenáre incidentov, pričom členovia tímu prechádzajú procesmi reakcie na incident v kontexte hypotetickej situácie. Cieľom je identifikovať medzery v pláne a zlepšiť koordináciu.
- **Simulácie a scénarizované testy:**
  - Vytvorenie realistických simulácií incidentov (napr. DDoS útok, ransomware) a vykonanie krokov v IRP v kontrolovanom prostredí, aby sa overila schopnosť tímu reagovať na reálne hrozby.
- **Technické testy:**
  - Testovanie technických opatrení, ako sú detekčné a reakčné mechanizmy (napr. SIEM, IDS/IPS) a zabezpečovacie nástroje, aby sa overilo, či správne identifikujú a reagujú na hrozby.
- **Audit a revízia:**
  - Pravidelné hodnotenie IRP vrátane analýzy minulých incidentov, revízie postupov a aktualizácie dokumentácie, aby sa zabezpečilo, že plán reflektuje aktuálne hrozby a zmeny v organizácii.
- **Red team vs. Blue team cvičenia:**
  - Red team simuluje útoky na systém, zatiaľ čo Blue team (defenzívny tím) reaguje a bráni infraštruktúru. Toto cvičenie umožňuje zhodnotiť efektívnosť IRP v praxi.

ZÁVER

- Ďakujeme za Váš čas
- Nasledujúci webinár na tému „ Riadenie kontinuity činností, zálohovanie, obnovu systémov po havárii a krízové riadenie“ 17.6.2025



NCC-SK

SLOVAKIA CYBERSECURITY COORDINATION CENTRE



Financované Európskou úniou

Vyjadrené názory a postoje sú názormi a vyhláseniami autorov a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za nich nepreberajú žiadnu zodpovednosť.

Ochrana vlastníckych práv

Všetky autorské práva k tomuto dokumentu sú vyhradené pre Kompetenčné a certifikačné centrum kybernetickej bezpečnosti (ďalej len „KCCKB“). Autorské práva k tomuto dokumentu má a autorské práva k tomuto dokumentu vykonáva KCCKB.

Vlastnícke práva tretích strán

Všetky ochranné známky a iné obdobné právne chránené označenia spomenuté v tomto dokumente sú výhradným vlastníctvom ich vlastníkov, ktorí sú, pokiaľ sa nejedná o KCCKB, v dokumente označení vo forme príslušnej citácie.

Akékoľvek kopírovanie či iné neoprávnené použitie celého dokumentu alebo jeho časti, v elektronickej alebo listinnej podobe, bez predchádzajúceho písomného súhlasu jeho autorov, napr. KCCKB, je zakázané. Porušenie vlastníckych a iných súvisiacich práv bude riešené v zmysle právnych predpisov Slovenskej republiky.

Limity informácií

Informácie obsiahnuté v tomto dokumente sú poskytované iba na informačné účely a bez akejkoľvek záruky, výslovnej či implicitnej. Názov KCCKB, logo KCCKB a ďalšie produkty a služby KCCKB sú ochrannými známkami KCCKB. Ostatné názvy spoločností, produktov alebo služieb môžu byť ochrannými známkami, alebo značkami služieb iných organizácií.