Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Riadenie udalostí a kybernetických bezpečnostných incidentov

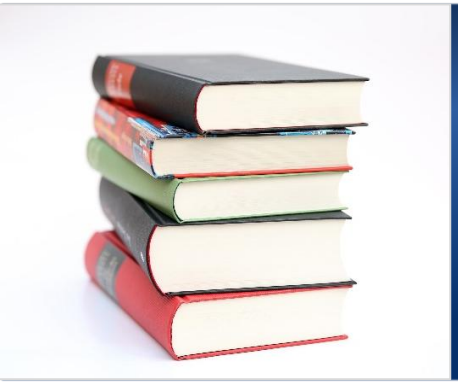
Organizačné opatrenia (Blok II)

Kurz: Manažér kybernetickej bezpečnosti vo verejnej správe

Milan Kubina

KC KYB UNIZA, https://kc.uniza.sk/

milan.kubina@fri.uniza.sk



Obsah

1. Riešenie kybernetických bezpečnostných incidentov (Incident Management)
2. Základné postupy pri spracovaní digitálnych stôp

Riešenie kybernetických bezpečnostných incidentov (Incident Management)

- Základné pojmy
  (udalosť, incident, bezpečnostný incident)
- Určenie závažnosti
- monitoring, hlásenia, logy
- SOC, metriky
- kategórie a príklady incidentov

Opakovanie ☺

- **Bezpečnostný atribút** informačného aktíva je vlastnosť alebo charakteristika, ktorá zabezpečuje ochranu tohto aktíva v súlade s požiadavkami bezpečnosti informácií.
- Tieto atribúty sú kritické pre zabezpečenie dôvernosti, integrity a dostupnosti informačných aktív.
- Medzi hlavné bezpečnostné atribúty patrí:
  - Dôvernosť (Confidentiality) – zabezpečuje, že informácie sú prístupné iba oprávneným osobám.
  - Integrita (Integrity) – zaručuje, že informácie nie sú zmenené alebo poškodené neoprávnenými osobami a že zostávajú presné a spoľahlivé.
  - Dostupnosť (Availability) – zabezpečuje, že informácie a systémy sú prístupné a použiteľné vtedy, keď sú potrebné.
  - Autentifikácia (Authenticity) – potvrdenie, že informácie sú skutočné a pochádzajú od správneho zdroja.
  - Nezávislosť (Non-repudiation) – zaručuje, že účastníci nemôžu poprieť svoje činnosti, ako napríklad odoslanie informácie alebo vykonanie akcie.

- **Tieto atribúty sú základom ochrany informácií a systémov v organizáciách a zabezpečujú ich bezpečné a správne fungovanie.**

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Udalosť

- Čokoľvek, čo sa stane alebo prebehne v určitom čase a priestore, bez ohľadu na to, či ide o bežnú, výnimočnú, pozitívnu alebo negatívnu situáciu.

- **Charakteristiky udalosti:**
  - má **čas a miesto**,
  - je to **skutočnosť alebo jav, ktorý nastal**,
  - môže byť neutrálna, priaznivá alebo nepriaznivá.

- **Príklady:**
  - bežná udalosť: narodenie dieťaťa, pracovné stretnutie, voľby,
  - prírodná udalosť: búrka, zemetrasenie, zatmenie Slnka,
  - spoločenská udalosť: koncert, svadba, výročie,
  - negatívna udalosť: požiar, havária, úraz...

Udalosť – pohľad IT

- Každý pozorovateľný jav, ktorý je možné jasne vnímať alebo detegovať v rôznych informačných systémoch a sieťach (NIST)
- Každá zmena stavu, ktorá je dôležitá pre správu konfiguračných položiek alebo pre poskytovanie IT služieb (podľa ITIL)
- Označenie výstrahy alebo upozornenia generovaného IT službou alebo monitorovacím nástrojom. (podľa ITIL)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Incident

- Neplánovaná alebo neočakávaná udalosť, ktorá spôsobí alebo môže spôsobiť narušenie normálneho chodu, služby, systému či procesu.

- **Charakteristiky incidentu:**
  - **nečakanosť** – nastane bez plánovania, nepredvídane,
  - **negatívny vplyv** – spôsobuje škodu, narušenie, ohrozenie, alebo aspoň riziko,
  - **vyžaduje reakciu** – často treba prijať opatrenia na obmedzenie alebo odstránenie následkov.

- **Príklady všeobecných incidentov:**
  - v doprave: dopravná nehoda, zrážka,
  - v IT: výpadok servera, útok hackerov,
  - v zdravotníctve: zlyhanie prístroja počas operácie,
  - v bezpečnosti: požiar, únik nebezpečnej látky....

Incident – pohľad IT

- Udalosť, ktorá má alebo môže mať nepriaznivý vplyv na fungovanie siete a informačných systémov, na poskytovanie základnej služby alebo IT služby.

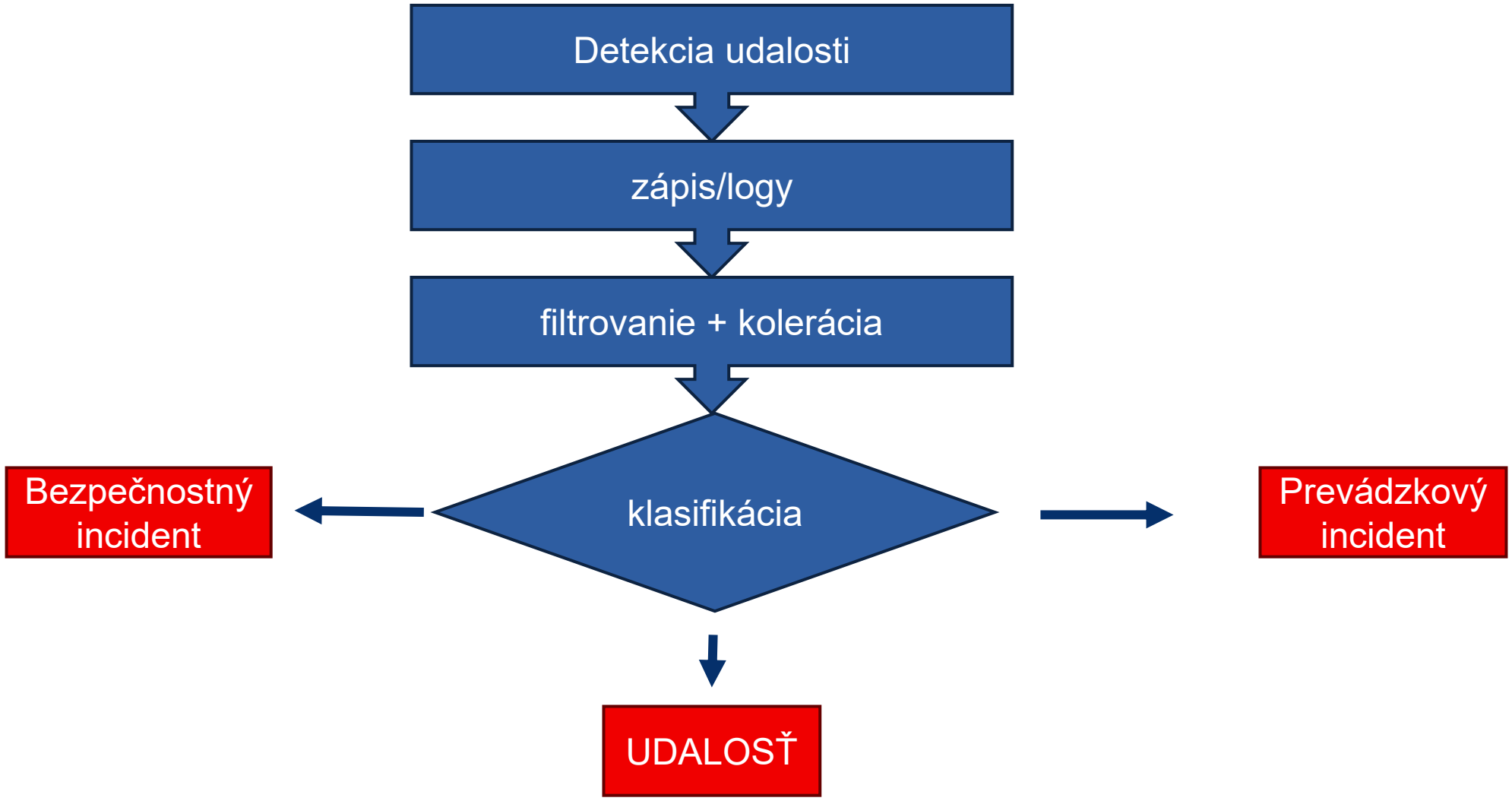
- **Rozdiely v terminológii:**
  - **Incident** = širší pojem, každá udalosť s negatívnym alebo potenciálne negatívnym vplyvom na IT/IT služby
  - **kybernetický incident** = súvisí s kybernetickou bezpečnosťou organizácie

Udalosť vs Incident

- udalosť = všeobecný pojem, zahŕňa všetko, čo sa stalo,
- incident = špeciálny typ udalosti s negatívnym alebo rizikovým dopadom, ktorý často vyžaduje nejakú reakciu.

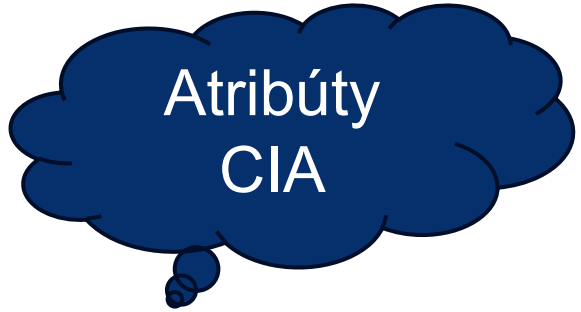
- Udalosť **nemusí nevyhnutne znamenať incident**, môže však poskytnúť indície, ktoré po vyhodnotení/analyzovaní môžu odhaliť nezvyklú alebo neočakávanú aktivitu

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE


Detekcia udalosti
zápis/logy
filtrovanie + kolerácia
klasifikácia
Bezpečnostný incident
Prevádzkový incident
UDALOSŤ

Kybernetický bezpečnostný incident (KBI)

- Následkom KBI je:
  - Strata dôvernosti dát,
  - Zničenie/poškodenie/strata dát
  - Prelomenie integrity systému
  - Obmedzenie alebo odmietnutie dostupnosti IT služby



Kybernetický bezpečnostný incident (KBI)

- Následkom KBI je:
  - nezvyklá alebo neočakávaná aktivita,
  - priestupok alebo riziko priestupku proti bezpečnostnej politike organizácie
  - Nesplnenie štandardných postupov
  - Porušenia záväznej metodiky/postupu
  - Použitie informačných aktív iným, než stanoveným spôsobom
  - ...

- PODVOD = úmyselne nekalá činnosť za účelom obohatenia sa resp. spôsobenie škody na cudzom majetku

Kybernetický bezpečnostný incident (KBI) - zákon 69/2018zz

- §3 písmeno m) – kybernetickým bezpečnostným incidentom je **udalosť ohrozujúca dostupnosť, pravosť ,integritu alebo dôvernosť** uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom sietí a informačných systémov.

- §3 písmeno n) – rozsiahlym kybernetickým bezpečnostným incidentom je kybernetický bezpečnostný incident, ktorý spôsobí **narušenie na úrovni presahujúcej schopnosť Slovenskej republiky naň reagovať**, alebo ktorý má významný vplyv aspoň na **dva členské štáty Európskej únie.**

Služby (NIS2)

- Kritické služby = okamžitá kritická infraštruktúra (energie, doprava, zdravie, voda, vláda).
- Základné služby = podporná infraštruktúra a hospodárstvo (pošty, odpady, výroba, potraviny, digitálne platformy).
  - Poštové a kuriérske služby
  - Odpadové hospodárstvo (zber, spracovanie, recyklácia)
  - Výroba, spracovanie a distribúcia potravín
  - Výroba (chemikálie, stroje, elektronika, dopravné prostriedky, zariadenia)

- ZS sú významné, ale s **nižšou bezprostrednou kritickosťou** – ich výpadok je vážny, no menej okamžitý a kritický

Kritická základná služba

Oblasť / sektor	Typ základnej služby	Príklady na Slovensku
Energetika	Výroba, prenos a distribúcia elektriny, plynu, ropy, tepla	Slovenské elektrárne, ZSE, SPP – distribúcia, Transpetrol
Doprava	Letecká, železničná, cestná a vodná doprava	ŽSR, ZSSK, Letisko M. R. Štefánika, NDS
Bankovníctvo a financie	Banky, infraštruktúra finančných trhov	Slovenská sporiteľňa, Tatra banka, Burza cenných papierov Bratislava
Zdravotníctvo	Poskytovanie zdravotnej starostlivosti	Univerzitná nemocnica Bratislava, VÚSCH Košice, laboratóriá
Zásobovanie vodou	Výroba a distribúcia pitnej vody, kanalizácia	BVS (Bratislavská vodárenská spoločnosť), VVS (Východoslovenská vodárenská spoločnosť)
Digitálna infraštruktúra	Internet, dátové centrá, cloud, DNS	Slovak Telekom, Orange, Swan, NIX.SK
Verejná správa	Orgány verejnej moci, štátne inštitúcie	Ministerstvá, Úrad vlády SR, Sociálna poisťovňa
Priemysel a potravinárstvo	Farmaceutická výroba, potraviny, kritické výrobky	Saneca Pharmaceuticals, Mondelēz Slovakia (Figaro), Duslo Šaľa

Identifikačné kritériá závažného narušenia fungovania prevádzkovateľa základnej služby

- **Príloha č. 1 vyhláška NBU 226/2025 Z. z.**
- 1. Úplný výpadok alebo nedostupnosť činnosti
  - 1.1 prevádzkovateľa kritickej základnej služby na viac ako 30 minút, alebo
  - 1.2 prevádzkovateľa základnej služby na viac ako 60 minút,
- 2. Narušenie alebo obmedzenie činnosti
  - 2.1 prevádzkovateľa kritickej základnej služby na viac ako 60 minút, alebo
  - 2.2 prevádzkovateľa základnej služby na viac ako 180 minút,
- 3. Ohrozenie dostupnosti, pravosti, integrity alebo dôvernosti údajov chránených podľa osobitného predpisu (Obchodný zákonník, zákon o bankách..)

Identifikačné kritériá závažného narušenia fungovania prevádzkovateľa základnej služby

- 4. Ohrozenie dostupnosti, pravosti, integrity alebo dôvernosti uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom sietí a informačných systémov, ktoré postihuje viac ako 25 000 osôb,
- 5. Spôsobenie hospodárskej straty vyššej ako 0,1 % hrubého domáceho produktu podľa údajov z bezprostredne predchádzajúceho rozpočtového roka,
- 6. Spôsobenie hospodárskej straty alebo hmotnej škody najmenej jednému užívateľovi viac ako 250 000 eur,
- 7. Vykonanie záchranných prác alebo výkon činností a opatrení súvisiacich s poskytovaním pomoci v tiesni alebo spôsobenie viac ako 100 zranených osôb vyžadujúcich lekárske ošetrenie alebo úmrtie aspoň jednej osoby

Identifikačné kritériá závažného narušenia fungovania prevádzkovateľa základnej služby

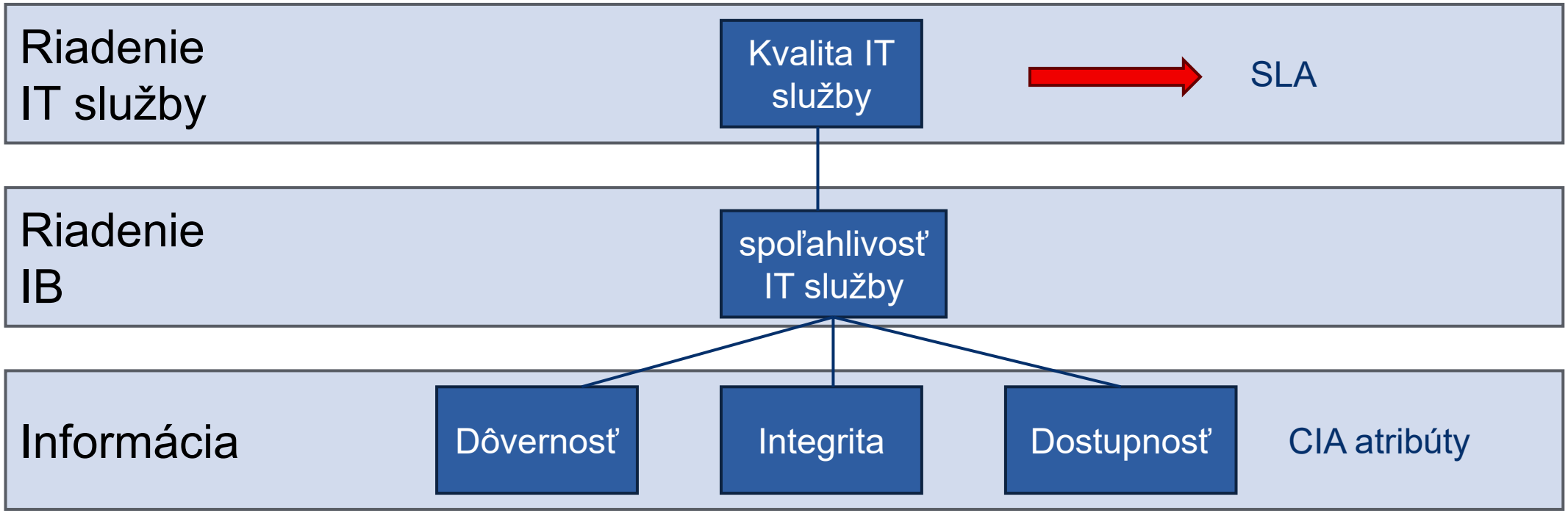
- 8. Udalosť,
  - 8.1 pri ktorej došlo k zjavne neoprávnenému prístupu do siete alebo informačného systému alebo došlo k znefunkčneniu siete alebo informačného systému a ktorá by mohla spôsobiť následky uvedené v prvom až siedmom bode,
  - 8.2 ktorá môže významne narušiť alebo ktorá narúša fungovanie iného prevádzkovateľa kritickej základnej služby, alebo
  - 8.3 ktorá je významným incidentom podľa osobitného predpisu(Čl. 3 vykonávacieho nariadenia Komisie (EÚ) 2024/2690, ktorým sa stanovujú pravidlá uplatňovania smernice (EÚ) 2022/2555) alebo incidentom podľa osobitného predpisu (Zákon č. 367/2024 Z. z. o kritickej infraštruktúre).

Kybernetický bezpečnostný incident vs kvalita IT služby

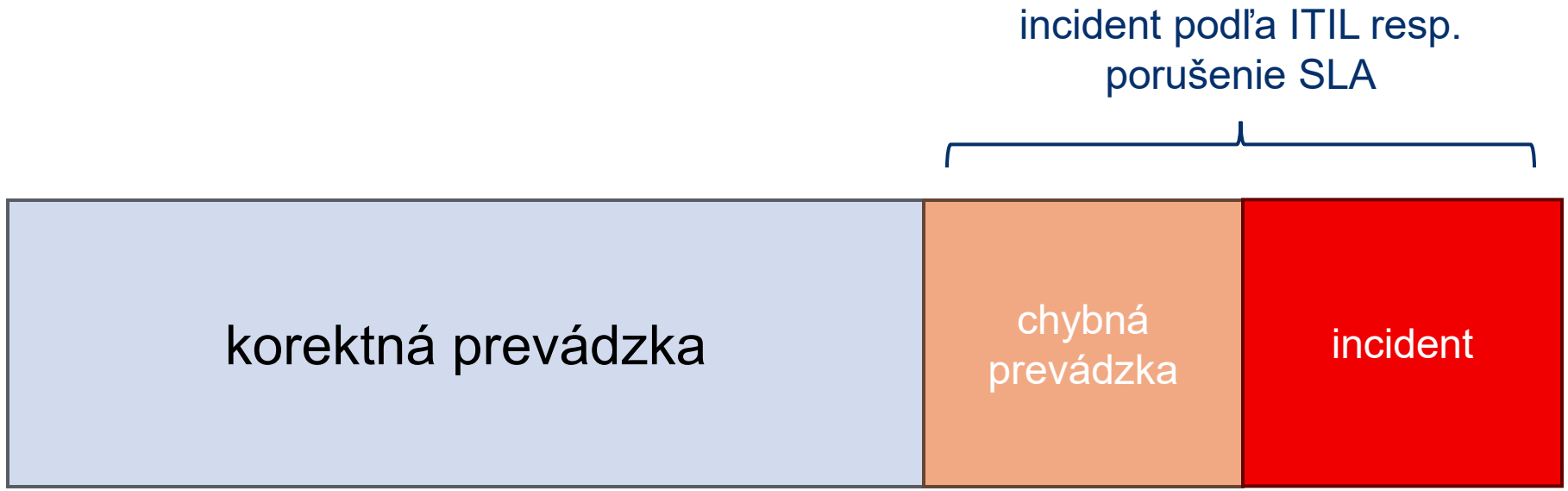
- Zníženie kvality alebo neplánované prerušenie IT služby (ITIL, ISO20000)
  - Incident je aj zlyhanie konfiguračnej položky aj keď zatiaľ neovplyvnilo službu resp. nemalo dopad na službu

- Jedna alebo viac nežiadúcich resp. neočakávaných bezpečnostných udalostí, u ktorých existuje vysoká pravdepodobnosť kompromitácie činnosti organizácie a ohrozenie bezpečnosti informácií (ISO 27001)

Incident v zmysle kvality IT služby



Incident v zmysle kvality IT služby



Požiadavky na zaznamenávanie udalostí/incidentov

- Zákon 69/2018 zz §20 ods.2
  - písmeno d) riadenie udalostí a kybernetických bezpečnostných incidentov
  - písmeno n) monitorovanie, zaznamenávanie a hlásenie udalostí

- Zákon 69/2018 zz §20 ods.4
  - b) detekciu kybernetických bezpečnostných incidentov,
  - c) evidenciu kybernetických bezpečnostných incidentov,
  - d) postupy riešenia a riešenie kybernetických bezpečnostných incidentov,
  - e) určenie kontaktnej osoby pre prijímanie a evidenciu hlásení,
  - f) pripojenie do komunikačného systému pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálneho systému včasného varovania

Prevádzkový monitoring

- **Prevádzkový monitoring** (niekedy aj **operatívny monitoring**) znamená **sústavné sledovanie a vyhodnocovanie prevádzky systémov, aplikácií a infraštruktúry** s cieľom zabezpečiť ich dostupnosť, výkon a bezpečnosť.

- Predmetom monitoringu sú:
  - **fyzické vlastnosti prostredia** – teplota, vlhkosť, prašnosť, hluk ...
  - **stav IT systémových ukazovateľov** – kapacita úložného priestoru, využitie operačnej pamäte...
  - **logické stavy** – stav OS, SW aplikácií, dostupnosť IT služieb, exspirácia certifikátov...

Bezpečnostný monitoring

- Vyhláška NBÚ č. 227/2025 – v časti rozsah bezpečnostných opatrení pre oblasti kybernetickej bezpečnosti podľa § 20 ods. 2 zákona o KB
  - položka Bezpečnostné opatrenia pre **monitorovanie, zaznamenávanie a hlásenie udalostí** podľa § 20 ods. 2 písm. n) zákona prijíma prevádzkovateľ základnej služby tak, že:
    - sú vytvárané a najmenej 12 mesiacov uchovávané relevantné prevádzkové a bezpečnostné logy, ktoré zachytávajú činnosti, výnimky, poruchy a iné relevantné prevádzkové a bezpečnostné udalosti, pričom bude zabránené zmene ich integrity a neoprávneným prístupom k nim
    - záznamy o činnostiach obsahujú informáciu o pôvodcovi vykonanej činnosti
    - siete, informačné systémy, programové prostriedky a aplikácie sú monitorované z hľadiska nezvyčajného správania a sú prijaté vhodné opatrenia na vyhodnotenie kybernetických bezpečnostných udalostí
    - sú prijaté a udržiavané mechanizmy overovania činností bezpečnostných funkcií a oznamovania nezvyčajného správania počas bežnej prevádzky, testovania a plánovanej údržby

Kategorizácia hlásení

	TRU	FALSE
Positive	TRU positive Alarm bol vygenerovaný a aj mal byť	FALSE positive Alarm bol vygenerovaný ale nemal byť
Negative	TRU negative Alarm nebol vygenerovaný a ani nemal byť	FALSE negative Alarm nebol vygenerovaný ale pritom mal byť

Kategorizácia hlásení

- **TRUE positive stav je želateľný stav monitoringu**
  - Ak sú korelačné pravidlá nevyladené, obsluha monitoringu je zahltená hláseniami a varovaniami
  - Ak sú pravidlá príliš silné, to má za následok „pochovanie“ aj dôležitých informácií, ktoré by mala obsluha monitoringu mať pre správne vyhodnotenie prevádzky
  - Počet chýb „TRUE negative“ vyjadruje mieru výkonnosti/vyladenia filtra

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Typy logov

- systémový log
- bezpečnostný log
- aplikačný log
- log udalostí
- log o chybách
- log prístupov
- log transakcií
- log...

Čo by sa nemalo logovať

- heslá
- šifrovacie kľúče
- zdravotné informácie
- informácie o platobných kartách
- osobné údaje

- Ak áno, treba to anonymizovať!

Normalizácia logov

- **Normalizácia logov** znamená proces, pri ktorom sa logy z rôznych zdrojov (servery, aplikácie, sieťové prvky, bezpečnostné zariadenia atď.) prevedú do **jednotného, štandardizovaného formátu**.
- **Prečo je potrebná?**
  - Rôzne systémy logujú v **odlišných štruktúrach** (formát dátumu, názvy polí, úrovne závažnosti, jazykové odlišnosti).
  - Bez normalizácie by bolo **ťažké logy porovnávať, filtrovať alebo analyzovať**.
  - Normalizované logy umožňujú rýchlejšie vyhľadávanie, koreláciu udalostí a efektívnejší **incident response**.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Normalizácia logov

- **Syntaktická normalizácia** logov znamená, že sa rôzne logy prevedú do **jednotného formátu na úrovni štruktúry (syntax)** – teda ako sú dáta zapísané, nie nutne čo presne znamenajú.
  - rôzne formáty zápisu (plain text, CSV, XML, JSON, syslog) sa rozparsujú a prevedú na spoločný dátový model,
  - zachová sa obsah (semantika sa zatiaľ nemusí meniť), ale všetko sa uloží do rovnakých polí.
- **Sémantická normalizácia** logov znamená, že sa zjednotí **význam (semantika) údajov**, nie iba ich zápis.
  - rôzne logy môžu mať odlišné pomenovania alebo hodnoty pre rovnakú vec – sémantická normalizácia tieto rozdiely preloží do jednotného „slovníka“.
    - Jednotné reporty – všetky logy používajú rovnaké kategórie
    - Jednoduchá korelácia udalostí – SIEM vie porovnať logy z rôznych zdrojov
    - Presnejšie alerty – pravidlá sa nemusia prispôsobovať každému výrobcovi

Rotácia logov

- **Rotácia logov** znamená proces, pri ktorom sa staré log súbory „odklonia“ bokom, aby sa uvoľnilo miesto pre nové záznamy.
  - Nový logovací súbor sa začne písať odznova (napr. system.log sa premenuje na system.log.1 a vytvorí sa nový system.log).
  - Zabraňuje sa tým nekonečnému rastu jedného súboru, ktorý by mohol spôsobiť problémy s výkonom alebo zaplnením disku.
- **Možnosti rotácie:**
  - Podľa veľkosti – napr. keď log dosiahne 100 MB, spraví sa rotácia.
  - Podľa času – napr. každý deň o polnoci sa vytvorí nový súbor.
  - Kombinácia – napr. max 50 MB alebo 1 deň, podľa toho, čo nastane skôr.

Archivácia logov

- **Archivácia logov** znamená dlhodobé uloženie logov, ktoré už nie sú aktívne potrebné pre operatívnu prevádzku, ale môžu byť potrebné pre:
  - forenznú analýzu (pri incidente)
  - compliance/súlad (napr. GDPR, zákon o KB, ISO 27001...)
  - audit (finančné systémy, prístupové logy)
- **Spôsoby archivácie:**
  - Kompresia – logy sa uložia ako .gz, .zip, aby zabrali menej miesta.
  - Presun do iného úložiska – napr. NAS, cloud
  - Špeciálne systémy – SIEM, WORM úložiská (Write Once, Read Many) pre nemenné dáta.

K logom

- event
  - bezpečnostnom kontexte znamená **udalosť,** teda akýkoľvek zaznamenaný jav v systéme alebo aplikácii, ktorý má určitý význam pre správu, prevádzku alebo bezpečnosť.
- alert
  - upozornenie alebo výstraha, ktorú vygeneruje systém, ak určitý **event (udalosť)** alebo kombinácia udalostí prekročí stanovené **pravidlá, prahy alebo podmienky**
- incident
  - potvrdený problém, ktorý má (alebo môže mať) negatívny dopad na organizáciu
  - **udalosť alebo sériu udalostí (events), ktoré ohrozujú dôvernosť, integritu alebo dostupnosť systémov, dát či služieb**.

SIEM

- **SIEM** = **Security Information and Event Management**.
  Je to softvérové riešenie, ktoré slúži na **zber, normalizáciu, analýzu a koreláciu logov a udalostí** z celej IT infraštruktúry organizácie
- SIEM je **centrálny mozog pre logy a bezpečnostné udalosti**, ktorý umožňuje **detegovať hrozby a reagovať na ne včas**

- **Výhody SIEM**
  - Jednotný prehľad o bezpečnostnej situácii.
  - Schopnosť rýchlo detegovať komplexné útoky.
  - Uľahčenie práce SOC (automatizácia, playbooky).
  - Podpora compliance a auditu.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Hlavné funkcie SIEM

- Zber a centralizácia logov z rôznych zdrojov: servery, siete, databázy, aplikácie, bezpečnostné zariadenia (firewally, IDS/IPS).
- Normalizácia a ukladanie
  - logy sa prevedú do jednotného formátu (syntaktická + sémantická normalizácia).
- Korelácia udalostí
  - SIEM spája udalosti z rôznych zdrojov a hľadá súvislosti.
- Monitoring a alerty
  - real-time detekcia incidentov a spúšťanie alarmov.
  - napojenie na SOAR nástroje (automatizovaná reakcia).
- Reporting a compliance
  - prehľadné dashboardy, audity a splnenie regulácií (ISO 27001, GDPR, NIS2, SOX).
- Forenzná analýza a vyhľadávanie
  - možnosť spätne analyzovať historické logy pri incidente.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

SOC

- **SOC** je skratka pre **Security Operations Center** – teda **centrum bezpečnostného dohľadu**. Je to špecializované pracovisko (tím + technológie), ktoré má na starosti:
  - monitorovanie bezpečnosti IT infraštruktúry,
  - detekciu a analýzu incidentov,
  - reakciu na kybernetické hrozby.

- Bezpečnostné „operačné centrum“, ktoré dohliada na IT infraštruktúru organizácie a chráni ju pred kybernetickými hrozbami.

Hlavné úlohy SOC

- **Monitoring**
  - nepretržité sledovanie logov, sieťovej prevádzky a udalostí (24/7).
- **Detekcia**
  - identifikácia podozrivých aktivít a kybernetických útokov.
- **Incident response**
  - analýza incidentov, návrh opatrení a koordinácia reakcie.
- **Forenzná analýza**
  - vyšetrovanie príčin útokov, zhromažďovanie dôkazov.
- **Reporting a compliance**
  - pravidelné reporty pre vedenie, dodržiavanie legislatívy (napr. GDPR, zákon o kybernetickej bezpečnosti).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Architektúra SOC

- **Ľudia (People)** – bezpečnostní analytici, incident response špecialisti, threat hunters.
- **Procesy (Processes)** – playbooky, incident response plány, SLA.
- **Technológie (Technology)**
  - SIEM (Security Information and Event Management),
  - SOAR (Security Orchestration, Automation and Response),
  - IDS/IPS,
  - EDR,
  - threat intelligence platformy.

Úrovne SOC (Tiering)

- **Tier 1 – Monitoring & Triage**
  - základný monitoring, filtrovanie falošných poplachov.
- **Tier 2 – Incident Analysis**
  - podrobnejšia analýza incidentov, hľadanie koreňovej príčiny.
- **Tier 3 – Threat Hunting & Forensics**
  - pokročilá analýza, lovenie hrozieb, reakcia na komplexné útoky.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Metriky pre riadenie KBI

- **Mean Time To Detect (MTTD)** – teda **priemerný čas na detekciu incidentu alebo problému**. Čím **nižšie MTTD**, tým rýchlejšie organizácia dokáže zareagovať.
- **Mean Time To Respond (MTTR) -** priemerný čas, za aký organizácia **začne reagovať na incident** po jeho detekcii.
- **Mean Time To Resolve (MTTR) -** priemerný čas potrebný na **úplné vyriešenie incidentu alebo problému** – od jeho vzniku až po definitívne uzavretie.
- Počet falošných poplachov resp. počet nesprávne identifikovaných incidentov
- Náklady na incident = celkové náklady na vyriešenie incidentu v organizácii
- Úroveň pripravenosti =hodnotenie úrovne pripravenosti organizácie na kybernetické útoky
- Počet vyriešených incidentov = % úspešne vyriešených incidentov
- atď.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Indikátory

- Indikátor je technický artefakt alebo nejaká pozorovateľná hodnota, ktorá nám naznačuje, že útok bezprostredne začal, práve prebieha alebo sa udial.
- **IoC – Indicator of Compromise (indikátor kompromitácie) -** znaky, že systém už bol napadnutý alebo kompromitovaný.
  - doména používaná pri phishingu,
  - neobvyklé záznamy v logoch
- **IoA – Indicator of Attack (indikátor útoku) -** znaky, že práve prebieha útok, alebo že sa niekto pokúša o zneužitie.
  - množstvo neúspešných prihlasovaní (brute force),
  - skenovanie portov.

TTP

- Taktiky – vysokoúrovňové ciele útoku (napr. úvodný prístup do siete..,)
  ..... PREČO
- Techniky – všeobecné metódy dosiahnutia týchto cieľov útoku (napr. phishing, latrálny pohyb.
  .....AKO
- Procedúry – špecifické implementácie alebo variácie používané v reálnych útokoch (variant malvéru, phishing kit...)
  .....ČO

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

MITRE ATT&CK

- **MITRE ATT&CK** (Adversarial Tactics, Techniques & Common Knowledge) je **globálne uznávaný rámec** vytvorený neziskovou organizáciou **MITRE**
- **databázu taktik, techník a postupov útočníkov (TTPs)** používaných v kybernetických útokoch.
  - Slúži ako „encyklopédia“ reálnych útokov, ktorú využívajú bezpečnostné tímy, SOC a red/blue/purple teamy.

- MITRE ATT&CK = otvorená databáza reálnych techník kybernetických útokov, ktorá pomáha organizáciám lepšie rozumieť útočníkom a zlepšiť obranu.

Hlavné časti MITRE ATT&CK

- **Tactics (taktiky)** – „prečo“ útočník koná → jeho cieľ (napr. získať prístup, presunúť sa v sieti, exfiltrovať dáta).
  - príklady: Initial Access, Persistence, Privilege Escalation, Defense Evasion, Exfiltration.

- **Techniques (techniky)** – „ako“ to robí → konkrétny spôsob, ktorým dosiahne cieľ.
  - príklady: phishing (Initial Access), credential dumping (Credential Access), Pass-the-Hash (Lateral Movement).

- **Sub-techniques (subtechniky)** – detailnejšie špecifikácie techniky.
  - napr. Phishing → spearphishing attachment, spearphishing link.

- **Mitigations (opatrenia)** – odporúčania, ako útokom predchádzať.
- **Detections (detekcia)** – návrhy, ako útok odhaliť (logy, senzory, monitoring).

MITRE ATT&CK matice

- **Enterprise Matrix** – útoky proti IT infraštruktúre (Windows, Linux, macOS, cloud, SaaS).
- **Mobile Matrix** – útoky na mobilné zariadenia (Android, iOS).
- **ICS Matrix** – útoky na priemyselné riadiace systémy (Industrial Control Systems).

Komunikácia KBI

- reputácia/reputačné riziko
- zamestnanci
- verejnosť
- partneri
- CSIRT
- orgány činné v trestnom konaní
- médiá
- atď.

- SMERNICE/USEMRNENIA

Kategórie/typy incidentov

- Útoky na web aplikácie
- DDoS/DoS útoky
- Odcudzené a stratené aktíva
- Rôznorodé chyby
- Zneužitie privilégií
- Sociálne inžinierstvo
- Prienik do systému
- Ostatné

PRÍKLADY typov incidentov

- **Malware** (škodlivý softvér) zahŕňa rôzne typy nežiaduceho kódu
  - Tento kód môže byť vo forme počítačových vírusov, trójskych koní alebo iných škodlivých programov
  - Cieľ: poškodiť systém alebo získať neoprávnený prístup
  - Vážna hrozba pre bezpečnosť a integritu počítačových systémov

- **Unknown/Suspicious**
  - Hlásenia o neznámych alebo podozrivých aktivitách v systéme
    - Môžu byť zaznamenané v sieťovej infraštruktúre
    - Môžu sa vyskytnúť aj na zariadeniach, ktoré sú pod monitorovaním
  - Vyžaduje ďalšiu analýzu na identifikáciu potenciálnych hrozieb

PRÍKLADY typov incidentov

- **System Status/Configuration**
  - Hlásenia týkajúce sa zmien alebo úprav v konfigurácii zariadení
    - Zahrnujú informácie o aktuálnom stave systémových zariadení
  - Prehľad o zmenách v nastaveniach a konfiguráciách

- **Reconnaissance Attempts**
  - Hlásenia o aktivitách zameraných na zistenie informácií o potenciálnych cieľoch v organizácii
  - Často predzvesťou budúcich útokov na sledované zariadenia alebo služby
    - Napr.: pokusy o skenovanie portov na identifikáciu zraniteľných miest
  - Môžu signalizovať prípravu na následné bezpečnostné incidenty

PRÍKLADY typov incidentov

- **Denial of Service**
  - Hlásenia o možných útokoch, ktoré sa zameriavajú na zablokovanie služieb
  - Cieľ → ochromiť služby poskytované cieľovým zariadením
    - Tento typ útoku zahŕňa odmietnutie služby (DoS) alebo útoky hrubou silou.
  - Útoky môžu viesť k výpadkom alebo úplnému nefunkčnému stavu systému alebo služby

- **Evasion**
  - Hlásenia o možnom zahladzovaní stôp po prieniku do zariadenia
    - Napr.: zneužitie chyby služby alebo zariadenia.
  - Po prieniku útočník skrýva svoje aktivity, aby predišiel detekcii
  - Cieľ → maskovať dôkazy o neoprávnenom prístupe a činnostiach

PRÍKLADY typov incidentov

- **Access / Authentication / Authorization**
  - Hlásenia o pokusoch o neoprávnený prístup k poskytovaným službám
    - Upozornenia na neoprávnené pokusy o autentizáciu alebo zmenu autentifikačných údajov
    - Hlásenia o pokusoch upraviť alebo získať autorizáciu práv na zariadenia alebo služby
  - Zahrňuje podozrenia na prezradenie, stratu, odcudzenie alebo odtajnenie autentifikačných informácií či zariadení

PRÍKLADY typov incidentov

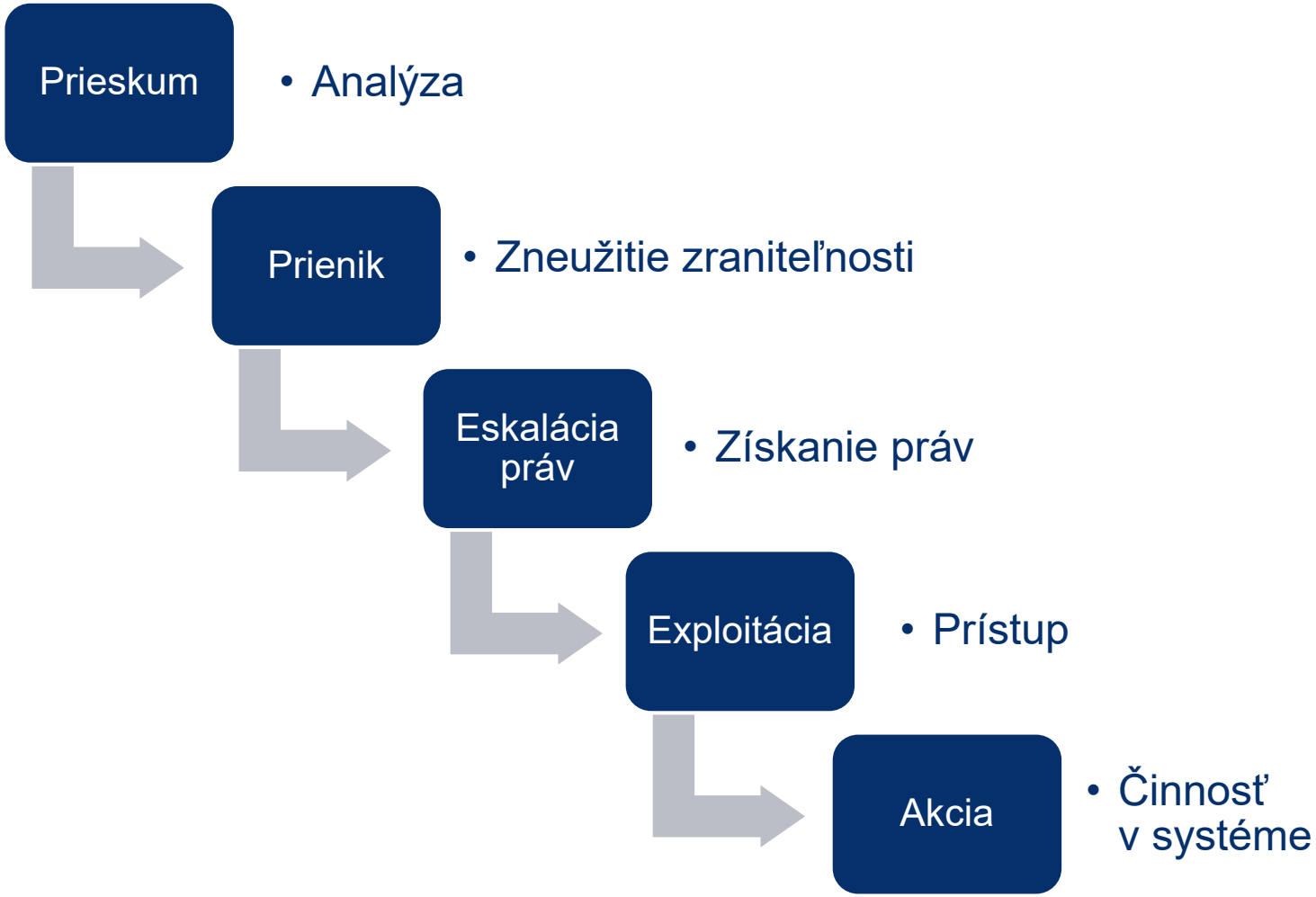
- **Application Exploit**
  - Hlásenia o možnom zneužití bezpečnostných chýb v poskytovanej službe alebo aplikácii
    - Upozornenia na potenciálne zraniteľnosti v zariadení, ktoré môžu byť zneužité
  - Naznačujú pokusy o vykonanie útoku prostredníctvom existujúcich chýb v systéme

- **PolicyViolations**
  - Hlásenia o porušeniach bezpečnostnej politiky organizácie
    - Upozornenia na hrozby alebo reálne priestupky proti akceptovateľnému používaniu politík
    - Hlásenia o nesplnení stanovených štandardných postupov a predpisov
  - Aj neoprávnené alebo neetické využívanie informačných aktív

PRÍKLADY typov incidentov

- **Viaczložkový incident**
  - Hlásenia o incidentoch, ktoré zahŕňajú viac než jednu kategóriu incidentu
    - Incidenty sa vyskytujú súčasne a pochádzajú z rovnakého zdroja
  - Viaczložkový incident môže zahŕňať rôzne typy útokov alebo bezpečnostných problémov v rovnakom čase

Proces útoku



Proces útoku

- **Prieskum**
  - Analyzovanie dostupných informácií o cieli
  - Cieľ:
    - Identifikovať slabé miesta
    - Potenciálne zraniteľnosti
  - Odhalenie možných bezpečnostných rizík

- **Prienik**
  - Dosiahnutie kritického bodu v systéme
    - Využiť existujúcu zraniteľnosť
  - Tento stav umožňuje zneužitie bezpečnostnej slabiny systému

Proces útoku

- **Eskalácia práv**
  - Pokus o získanie privilegovaných oprávnení v systéme
  - Cieľ: získať prístup k vyšším právam používateľa
  - Zahŕňa neautorizovaný pokus o získanie privilégií na úrovni administrátora

- **Exploitácia**
  - Využitie existujúcej zraniteľnosti v systéme
  - Cieľ: získať neoprávnený prístup k citlivým údajom alebo systémovým funkciám
    - Obísť bezpečnostné mechanizmy a získať prístup bez autorizácie

Proces útoku

- **Akcia**
  - Realizácia špecifických akcií v systéme zo strany útočníka
  - Cieľ: dosiahnutie zamýšľaného výsledku útoku
  - Útočník vykonáva kroky, ktoré vedú k naplneniu jeho cieľov

- **Maskovanie**
  - Evasion
  - Útočník vykonáva priebežné činnosti počas celého útoku
  - Cieľ: minimalizovať riziko detekcie a udržať útok neviditeľný
  - Útočník sa snaží zamaskovať svoje kroky a zabrániť odhaleniu

Proces riešenia KBI

- NIST a ISO/IEC 27035:2011

Odozva na incident

- Incident Response
- Proces reakcie na bezpečnostný incident
  - Preddefinovaná reakcia
  - Formalizovaná reakcia
  - Otestovaná reakcia
- Ciele:
  1. **Obnova funkčnosti** poškodených informačných aktív a návrat k normálnemu chodu činností
  2. **Zabezpečenie právnej nápravy** a zber digitálnych dôkazov na podporu právnych krokov proti páchateľovi

Formalizovaný proces riešenia incidentov

1. **Detekcia**
   - Odhalenie incidentu
     - Testovanie
     - Monitoring
     - Indikácia
     - Predbežná analýza
     - Posúdenie
     - Kategorizácia

2. **Reakcia**
   - Odozva na incident
     - Horizontálna eskalácia
       - Funkčné eskalačné procesy → úroveň odborných útvarov
     - Vymedzenie a izolácia
     - Odstránenie následkov
     - Vertikálna eskalácia
       - Hierarchické eskalačné procesy → úroveň manažmentu, autority (ústredný orgán), tretie strany, komunikácia cez médiá
     - Náprava škôd

3. **Post-incidentné aktivity**
   - Záverečná správa
   - Forenzná analytika
   - Prevencia
   - Právne následky
   - Plánovanie a príprava

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Zdroje na detegovanie incidentu

- **Subjektívne vnímanie incidentu:**
  - Hlásenia od používateľov o pozorovaní neobvyklej aktivity alebo udalosti
    - Napr.: pokusy v oblasti sociálneho inžinierstva
    - Prípad, kedy sa zistia neoprávnené prístupy k informáciám alebo dátam
- Identifikácia sekundárnych následkov incidentu:
  - Pozorovanie nezvyčajného zvýšenia záťaže systému
  - Nárast objemu sieťovej prevádzky alebo spotreby energie
  - Spomalenie odozvy systému alebo iné technické problémy, ktoré môžu naznačovať incident

Zdroje na detegovanie incidentu

- **Formálne zdroje detekcie incidentu:**
  - Hlásenia z procesov riešenia bezpečnostných incidentov
    - Hlásenia z prevádzkových a bezpečnostných monitorovacích systémov
    - Informácie poskytnuté jednotkami CSIRT
  - Oznámenia z externého prostredia
    - Hlásenia od orgánov činných v trestnom konaní
    - Správy z médií alebo informácie priamo od dotknutých osôb a subjektov
  - Výsledky vykonaného testovania alebo zistenia počas auditu

Plán reakcie na incident

- CSIRP - Computer Security Incident Response Plan
- Podrobný popis procesov týkajúcich sa riadenia a riešenia bezpečnostných počítačových incidentov
- Diagnostická matica, ktorá slúži na urýchlenie rozhodovania a poskytuje podporu pre menej skúsený personál
- Musí obsahovať minimálne nasledujúce procesy:
  - Profilovanie systémov a určenie kritickosti procesov v rámci organizácie
  - Definovanie spúšťačov (triggers), identifikácia zdrojov indikácií a určenie spôsobov notifikácie incidentov
  - Komunikačná matica a detailný popis hlavných postupov pre fázu reakcie na incident
  - Podrobný popis spôsobu obsluhy incidentov, rozdelený podľa jednotlivých kategórií, s odkazmi na bázu znalostí (ak je to možné)
  - Popis hlavných post-incidentných aktivít, ktoré je potrebné vykonať po incidente
  - Klasifikácia hlásení a kategorizácia incidentov s ohodnotením ich závažnosti
  - Definovanie spôsobu, termínov a zodpovedností za aktualizáciu a testovanie plánu
  - Pripravenosť na použitie CSIRP v stresových situáciách, napríklad pomocou checklistu na rýchlu orientáciu a rozhodovanie

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Riadenie prístupov – zásady a terminológia

- **Riadenie prístupu:**
  - Schopnosť určenej entity (subjektu) kontrolovať a regulovať prístup k prostriedkom
    - Ich povoľovaním alebo zakazovaním
- **Subjekt:**
  - Používateľ alebo proces, ktorý žiada prístup k systémovým prostriedkom alebo údajom
- **Objekt:**
  - Konkrétny prostriedok, ku ktorému sa subjekt pokúša získať prístup, pričom objektmi môžu byť napríklad súbory, databázy alebo aj procesy v systéme
- Keď sa subjekt pokúša získať prístup k objektu:
  - Nevyhnutné rozhodnúť o povolení alebo zamietnutí prístupu
- Tento proces rozhodovania je realizovaný prostredníctvom bezpečnostného mechanizmu:
  - **Riadenie prístupov**

Riadenie prístupov – politiky

- **Voliteľné riadenie prístupu**:
  - Politika určená vlastníkom objektu (tým, kto objekt vytvoril)
  - Tento model neberie do úvahy použitie už raz získaných dát
- **Povinné riadenie prístupu**:
  - Politika definovaná systémom, kde sú objekty a subjekty priradené k bezpečnostným označeniam
    - Na základe týchto označení bezpečnostný mechanizmus rozhoduje o oprávnenosti prístupu
  - Striktne definované pravidlá určujú prístup medzi rôznymi bezpečnostnými úrovňami

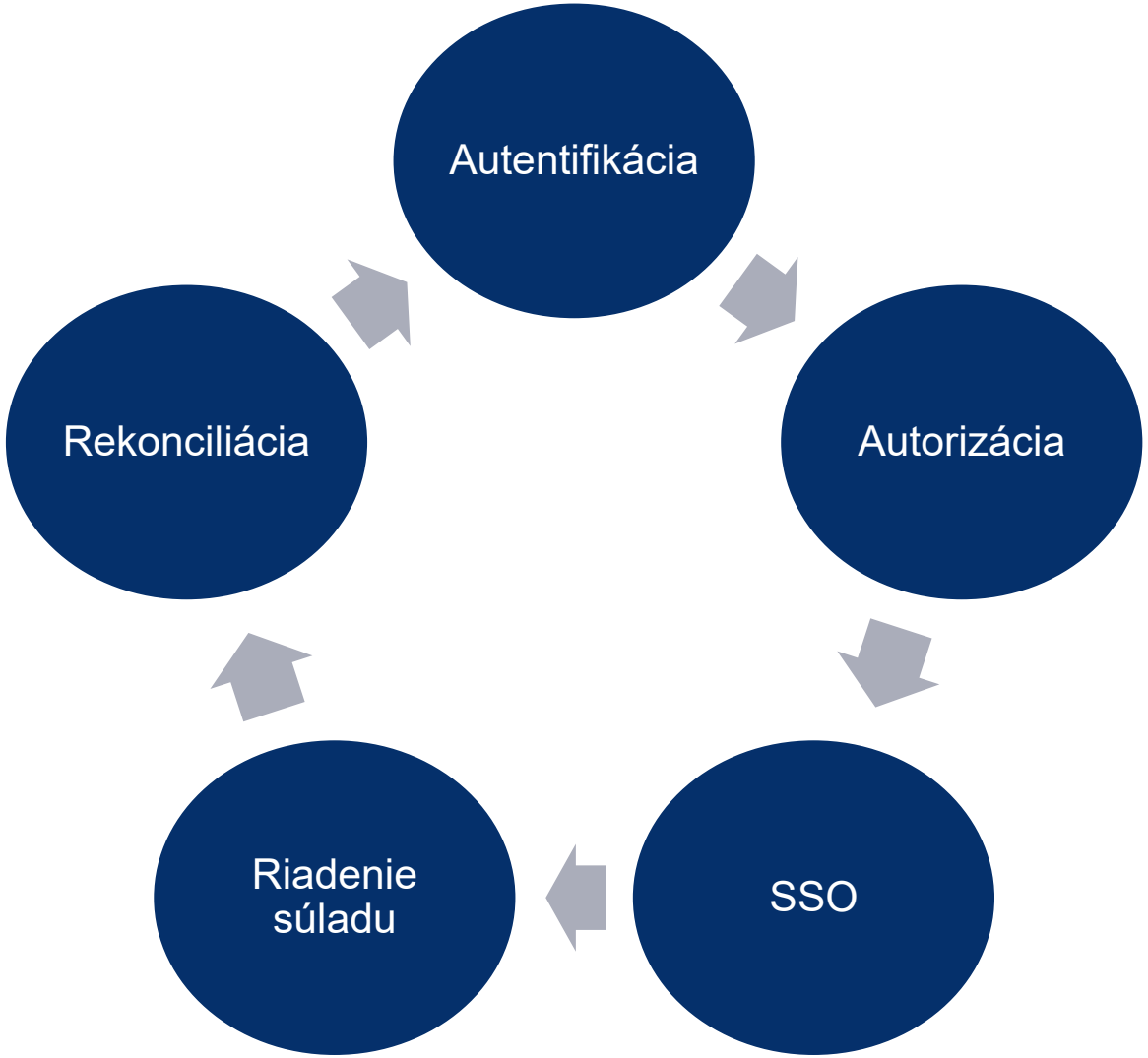
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Riadenie prístupov – politiky

- **Riadenie prístupu na základe rolí (RBAC):**
  - Role-Based Access Control
  - Používateľom sú priraďované role, ktoré obsahujú oprávnenia na vykonávanie konkrétnych činností
  - Používateľ môže mať viacero rolí, čo umožňuje flexibilnejšie nastavenie politiky v porovnaní s ACL
    - Access Control List
  - V rozsiahlejších prostrediach môže byť implementácia RBAC náročná, pretože každá rola býva špecifická pre jednotlivé systémy

Životný cyklus identity

Proces prideľovania, používania a odoberania identifikačných údajov v elektronickej forme, ktoré jedinečne reprezentujú fyzickú osobu alebo inú konkrétnu entitu v kybernetickom priestore.



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Životný cyklus identity

Identifikácia

- Proces, pri ktorom sa používajú osobné identifikačné údaje
- Údaje sú elektronické a slúžia na jednoznačné rozpoznanie subjektu
- Identifikačné údaje reprezentujú buď fyzickú osobu, alebo právnickú osobu
- Tento proces je kľúčový pre autentifikáciu a určenie konkrétneho subjektu v systéme

Autentifikácia, Autentizácia

- Elektronický proces, ktorý slúži na potvrdenie identity
- Umožňuje overiť elektronickú identifikáciu fyzickej alebo právnickej osoby
- Potvrdzuje pôvod a integritu údajov v elektronickej forme
- Cieľ → zabezpečiť, že údaje alebo identita sú správne a dôveryhodné

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Životný cyklus identity

Validácia

- Proces, ktorý slúži na overenie platnosti elektronických podpisov alebo pečatí
- Potvrdzuje, že elektronický podpis alebo pečať sú legitímne a platné
- Zabezpečuje, že podpis alebo pečať neboli zmenené a sú právne záväzné

Autorizácia

- Proces, pri ktorom sa pridelia oprávnenia na vykonanie transakcie alebo úkonu
- Vždy nasleduje po úspešnej autentizácii
- Využíva výsledky autentizácie na určenie, aké práva a oprávnenia môžu byť používateľovi priradené

Rekonciliácia

- Proces, ktorý umožňuje v reálnom čase porovnávať zoznam skutočne vytvorených prístupov v počítačových systémoch s požadovaným stavom udelených prístupov

Základné postupy pri spracovaní digitálnych stôp

- Základné pojmy (stopa vs. dôkaz, digitálna stopa)
- Digitálna forenzná analýza
- Postupy spracovania digitálnych stôp

Stopa vs. dôkaz

- **Stopa**

  akákoľvek zmena v materiálnom prostredí alebo vo vedomí človeka, ktorá príčinne alebo aspoň miestne a časovo, súvisí s vyšetrovanou udalosťou, obsahuje kriminalisticky alebo trestnoprávne relevantnú informáciu, je zistiteľná, zaistiteľná a využiteľná pomocou dostupných kriminalistických, prírodovedných a technických metód, prostriedkov a postupov.

- **Dôkaz**

  získané, agregované informácie o stopách, ktoré môžu byť použité na podporu tvrdení alebo aj na ich zamietnutie.

  - **Digitálne dôkazy =** informácie alebo údaje, uložené alebo zasielané v binárnej forme, na ktoré sa možno opierať v dôkaznom konaní

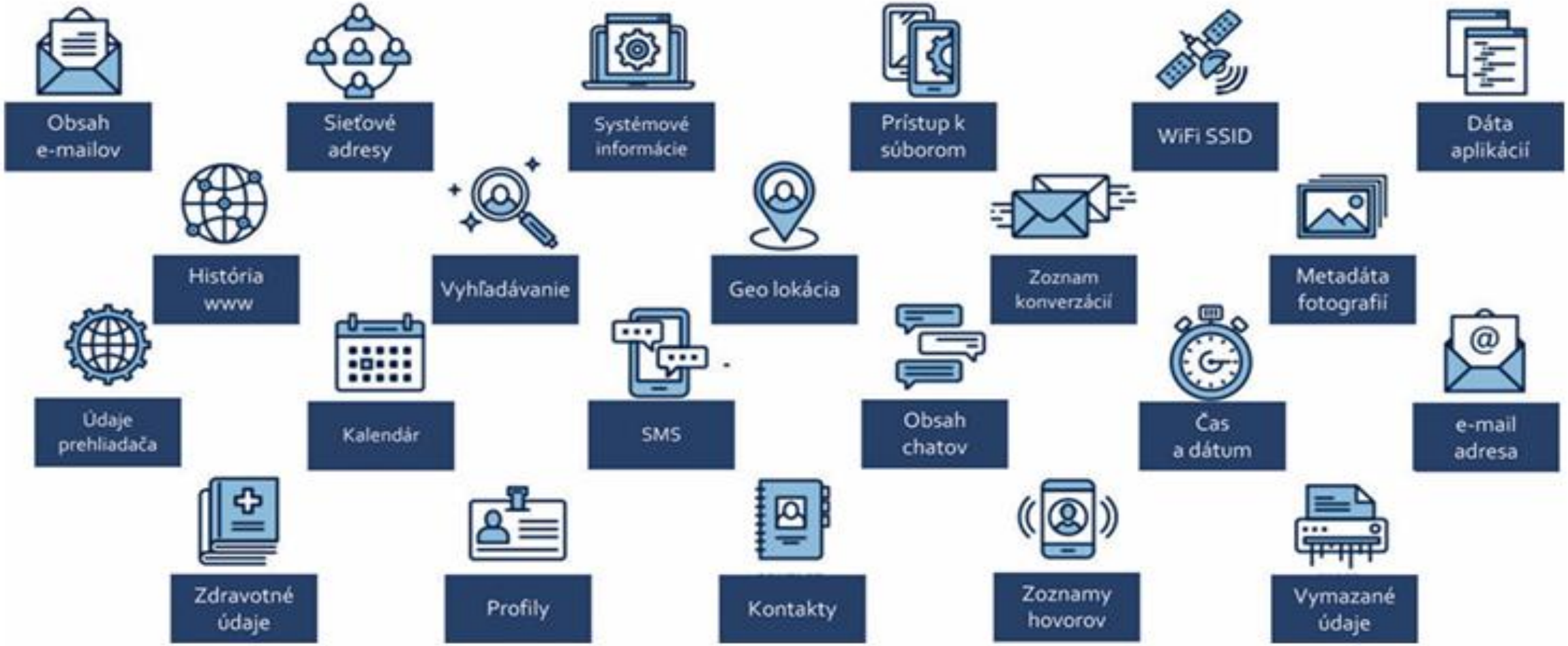
- Z tohto pohľadu všetko, čo považujeme za relevantné pre konkrétny problém, je zároveň stopou a potenciálnym dôkazom súčasne

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Digitálna stopa, digitálny tieň

- Jedinečná množina vystopovateľných digitálnych aktivít, činností, príspevkov a komunikácie na internete a/alebo pomocou zariadení informačných a komunikačných technológií
  a) **Aktívna –** údaje, ktoré používateľ odosiela do kybernetického priestoru úmyselne, s istým zámerom (napr. e-maily, príspevky na sociálnych sieťach, obsah chatov a SMS správ, história internetových prehliadačov, história vyhľadávania, metadáta fotografií, záznamy o používaní platobných kariet a mnohé iné)
  b) **Pasívna –** dáta, ktoré používateľ zanecháva nechtiac pri online činnostiach (napr. IP adresa, geografická lokácia zariadenia, cookies a pod.)
- Reprezentované vo:
  a) **Fyzickej forme –** zobrazenie údajov na rozhraní konkrétneho zariadenia, alebo údajov na fyzických dátových médiách
  b) **Logickej forme –** týka sa virtuálneho zobrazenia a interpretácie údajov

Digitálne stopy – príklady



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Digitálna forenzná analýza

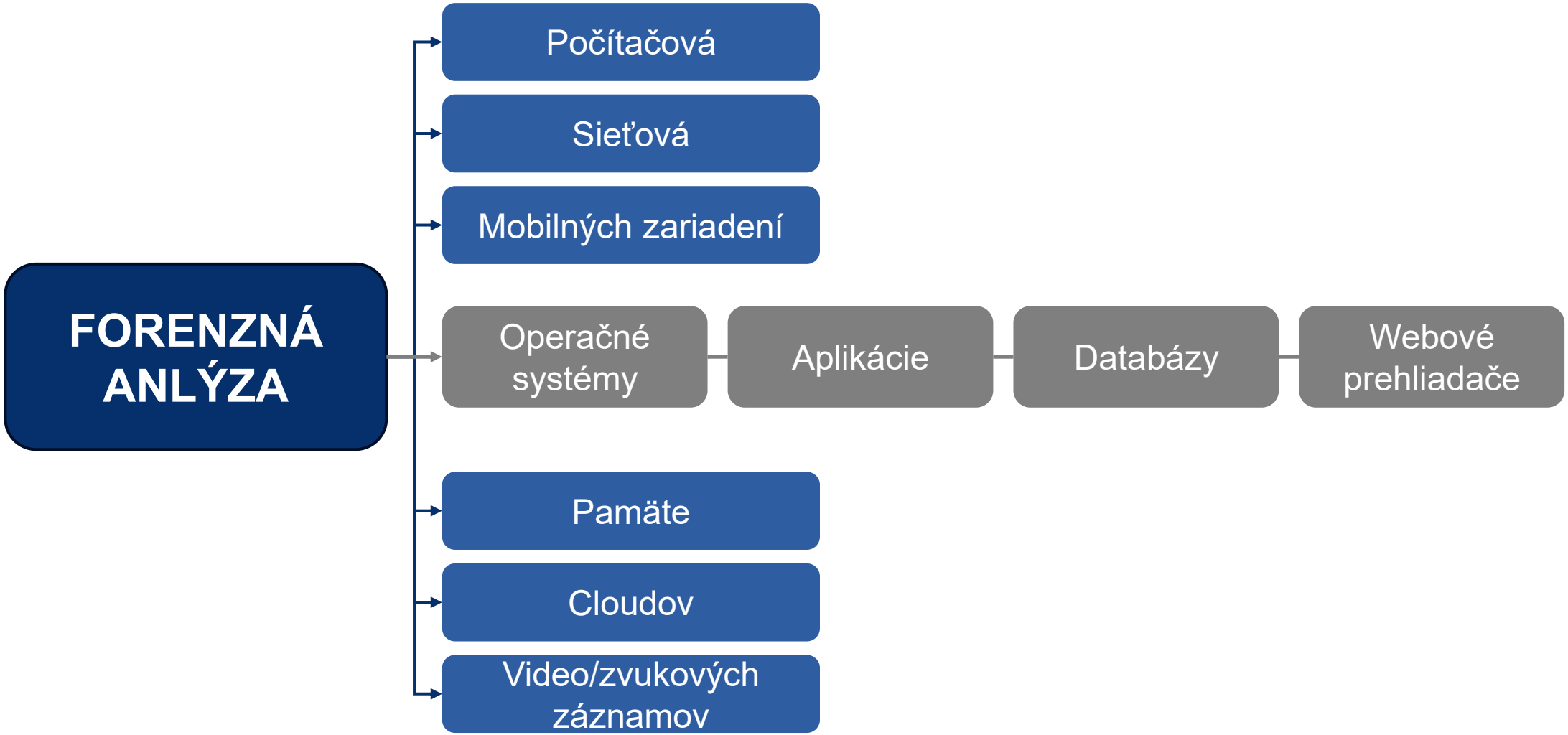
- Viacstupňový proces začínajúci identifikáciou digitálnych médií zo scény ako potenciálnych stôp končiaci vo fáze, v ktorej sú predložené ako dôkazy súdnym znalcom na súde v rámci civilného alebo trestného konania
- Proces reakcie na incident od identifikácie a analýzy digitálnych stôp až po predloženie digitálnych stôp buď vrcholovému vedeniu, alebo súdu pre účely civilného alebo trestného konania
- **Využitie:** nielen pre účely civilného alebo trestného konania, ale aj pre riešenie bezpečnostného incidentu
- **Ciele:** pomoc pri obnove, analýze a uchovaní materiálov; návrh postupov na mieste činu; zber a duplikácia údajov; pomoc pri identifikácii digitálnych stôp; vytvorenie počítačovej forenznej správy

Fázy digitálnej forenznej analýzy

Identifikácia	Identifikácia účelu vyšetrovania a potrebných zdrojov; prostredia; vyhľadávanie, rozpoznávanie a dokumentáciu potenciálnych digitálnych stôp
Zaisťovanie a zber	Zhromažďovanie údajov z digitálnych zariadení; zhromažďovanie zariadení, ktoré obsahujú potenciálne digitálne stopy
Uchovanie	Uloženie digitálnych stôp na vhodnom médií; zaistenie integrity zaistených digitálnych stôp
Vyťažovanie	Extrakcia z digitálnych stôp; redukcia a filtrovanie údajov; obnova súborov a získavanie údajov
Analýza	Identifikujú sa nástroje a techniky, ktoré sa majú použiť; prioritizácia, filtrácia, korelácia digitálnych stôp; interpretácia výsledkov a vyhodnotenie hypotéz
Prezentácia	Sumarizácia a vysvetlenie výsledkov; predloženie výsledkov zadávateľovi

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Digitálna forenzná analýza – typy



Digitálna forenzná analýza – metódy zaobstarania

Metódy zaobstarania digitálnych stôp:

- **Zber (alebo tiež zhromažďovanie) –** proces nadobudnutia, v ktorom sú zariadenia a fyzické položky, ktoré môžu obsahovať potenciálne dôkazy, odstránené z pôvodného umiestnenia (napr. z pracoviska podozrivého) a prenesené do laboratória, alebo do iného kontrolovaného prostredia na neskoršiu analýzu
- **Akvizícia (získavanie) –** proces nadobudnutia, ktorý zahŕňa vytvorenie kópie digitálnych dôkazov v rámci definovanej množiny (napr. kompletného obsahu úložiska, logického oddielu disku, vybraných súborov, dump pamäte, atď.) a dokumentovanie použitých metód a vykonaných činností pričom produktom akvizície je digitálna kópia potenciálnych dôkazov

- Špecifické činnosti – identifikácia, uchovanie

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Manipulácia s digitálnymi stopami

Požiadavky a pravidlá **pri zbere**:

- **Požiadavka prípustnosti (admissible) -** digitálne stopy musia pred predložením súdu zodpovedať určitým právnym pravidlám
- **Požiadavka autentickosti –** musí byť zachová neporušiteľnosť (integrita) digitálnych stôp a zachovaná reťaz dôvery (chain of custody)
- **Požiadavka kompletnosti –** digitálne stopy musia popisovať celý skutok, nielen osobitnú perspektívu

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Manipulácia s digitálnymi stopami

Požiadavky a pravidlá **pri zbere**:

- **Požiadavka spoľahlivosti** – postupmi a nástrojmi na zhromažďovanie, preskúmanie, analýzu, uchovávanie a vyhodnotenie digitálnych stôp musí byť možné replikovať rovnaké výsledky v priebehu času. Postupy nesmú spochybňovať pravosť dôkazov a závery vyvodené po analýze
- **Požiadavka vierohodnosti** – digitálne stopy by mali byť jasné, ľahko pochopiteľné a vierohodné. Verzia digitálnych stôp predložených pred súdom musí byť spätne spojená s pôvodnými binárnymi digitálnymi stopami, inak nie je možné zistiť, či boli digitálne stopy vykonštruované

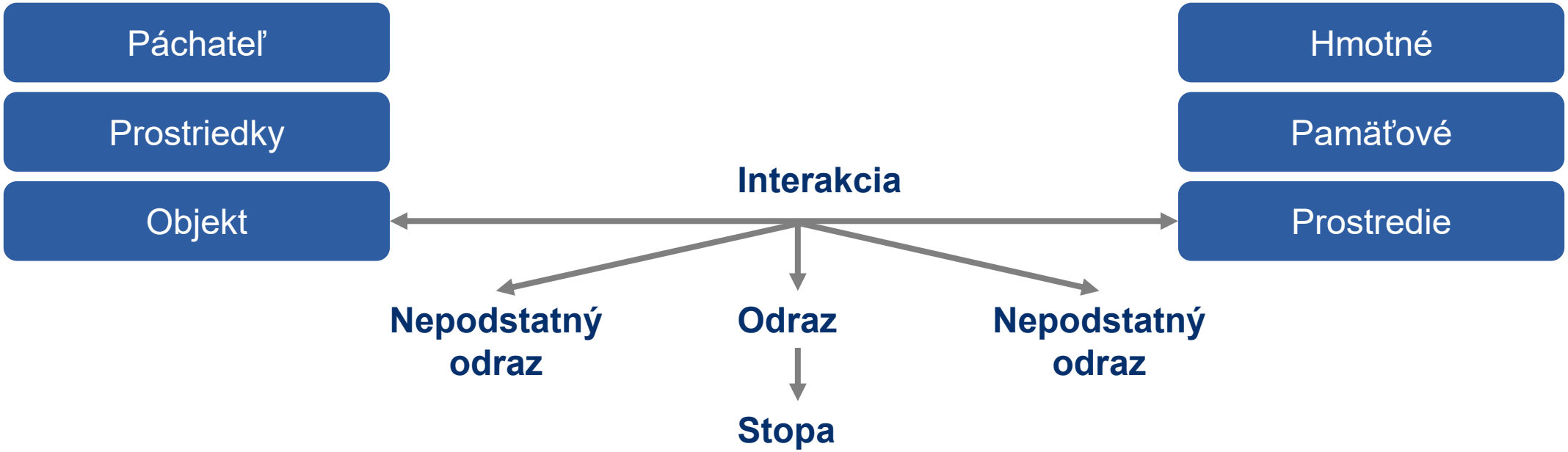
Princípy digitálnej forenznej analýzy

- Výmena stôp (Evidence Exchange)
- Charakteristika stôp (Evidence Characteristics)
- Forenzná korektnosť (Forensic Soundness)
- Autentickosť (Authentication)
- Reťaz dôvery (Chain of Custody)
- Integrita stôp (Evidence Integrity)
- Objektivita (Objectivity)
- Opakovateľnosť (Repeatability)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

1) Výmena stôp (Evidence Exchange)

- Dr. Edmund Locard – francúzsky vedec, základný forenzný princíp
- **Locardov princíp výmeny =** kontakt dvoch objektov zanecháva na objektoch stopy, tzn. že keď sa vo fyzickom svete dva objekty dostanú do kontaktu (interakcie), tak sa nejaký materiál prenáša z jedného na druhý a naopak. Dochádza k niekoľkým odrazom tejto interakcie a niektoré sa uchovávajú.



2) Charakteristika stôp (Evidence Characteristics)

- **Nehmotnosť** – dáta a informácie sú nehmotné, ale je možné ich zhmotniť, napríklad uložením na hmotný nosič, vytlačením na papier
- **Latentnosť digitálnych stôp** – digitálne stopy sú neviditeľné. Záznamy na hmotnom nosiči sú neviditeľné. Vidieť môžeme fotografie, videá, dokumenty, ale nevidíme reálne údaje a informácie, len ich výsledok vnímateľný zmyslami
- **Časová trasovateľnosť** – digitálne stopy obsahujú časové pečiatky. Každá činnosť sa zaznamenáva s uložením aj času vykonania (napr. vytvorenie súboru)
- **Vysoká obsažnosť** – môžu mať vysokú informačnú hodnotu o aktivitách na zariadení, ako aj samotnom používateľovi, či útočníkovi
- **Veľký dátový objem** – súčasne počítačové systémy spracúvajú veľké množstvo údajov. Neustále rastú požiadavky na operačnú pamäť. Týmto narastá nielen objem samotných používateľských údajov, ale aj údajov potrebných k fungovaniu operačného systému, metadát a pod. S týmto priamo súvisí aj kapacitná a finančná náročnosť pri zaistení a uchovávaní digitálnych stôp a ich použitia v rámci trestného alebo iného konania.

2) Charakteristika stôp (Evidence Characteristics)

- **Extrémna dynamickosť prostredia –** ovplyvňuje životnosť digitálnych stôp. Životnosť digitálnych stôp závisí od média, na ktorom sú uložené. Veľká časť pamätí, resp. ich častí (registre) je náchylná na zmeny. To spôsobuje, že niektoré digitálne stopy majú životnosť rádovo v tisícinách sekundy
- **Heterogénnosť a komplexnosť prostredia –** počítačové systémy ako také sú heterogénne, existuje veľké množstvo rôznych hardvérových súčastí, operačných systémov, softvérového vybavenia a pod. To spôsobuje veľké množstvo rôznych zdrojov digitálnych stôp
- **Veľký geografický rozsah priestoru –** existencia Internetu a následne aj cloudových služieb spôsobila, že relevantné digitálne stopy sa môžu nachádzať na dátových nosičoch v rámci celého sveta. Vysoký stupeň ochrany dát sťažuje alebo znemožňuje prácu s digitálnymi stopami
- **Originálnosť–** dátové nosiče, súbory, resp. iné záznamy je možné jednoducho kopírovať bez straty, resp. poškodenia údajov

3) Forenzná korektnosť (Forensic Soundness)

- Digitálne forenzné vyšetrovanie:

  dodržanie zavedených zásad, štandardov a procesov = korektné vyšetrovanie

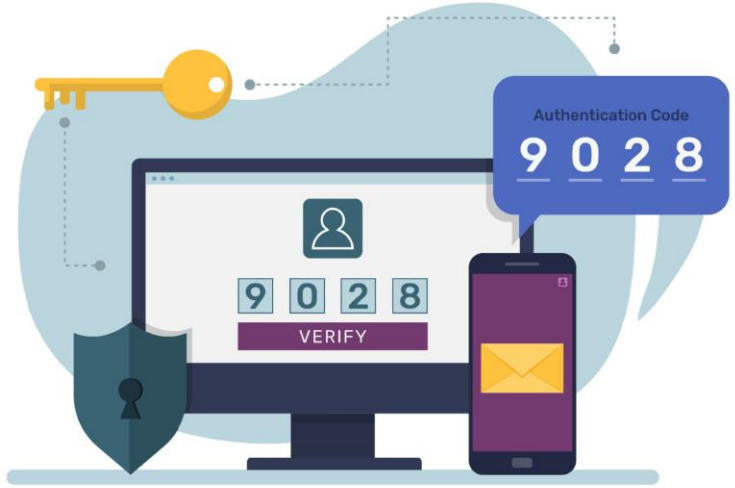
- Použite metód pozostávajúcich zo systematického pozorovania, merania a experimentu a formulácie, testovania a úpravy hypotéz

- Digitálne forenzné vyšetrovanie je korektné, **AK** sa nijakým spôsobom nezmení pôvodný zdroj digitálnych stôp a je úplne reprodukovateľné treťou stranou

4) Autentickosť (Authentication)

- Autentickosť = overiteľnosť pravosti digitálnych stôp

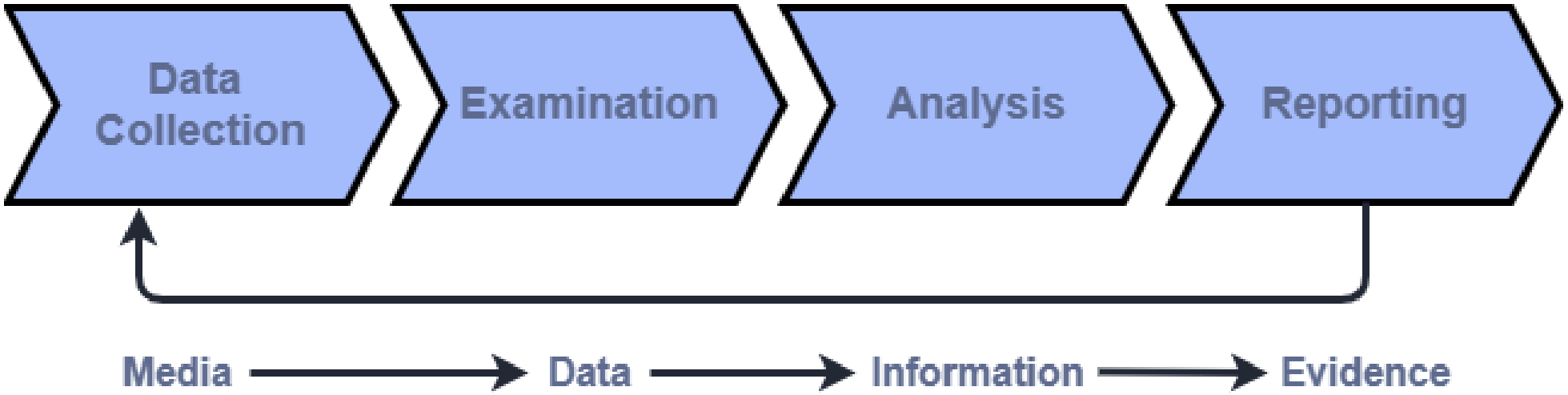
- Dvojkrokový proces:
  1. Preskúmanie skutočnosti, že predložené digitálne stopy sú tie isté, ako tie, ktoré boli získané pri zaistení
  2. Určenie dôkaznej hodnoty digitálnych stôp



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

5) Reťaz dôvery (Chain of Custody)

- Dokumentácia popisujúca celý proces získavania, prenosu, manipulácie a ukladania fyzických alebo digitálnych stôp
- Tento životný cyklus začína, keď osoba (napr. forenzný analytik) zaistí digitálnu stopu a končí vyriešením bezpečnostného incidentu, resp. odovzdaním výsledkov vyšetrovania príslušným orgánom



6) Integrita stôp (Evidence Integrity)

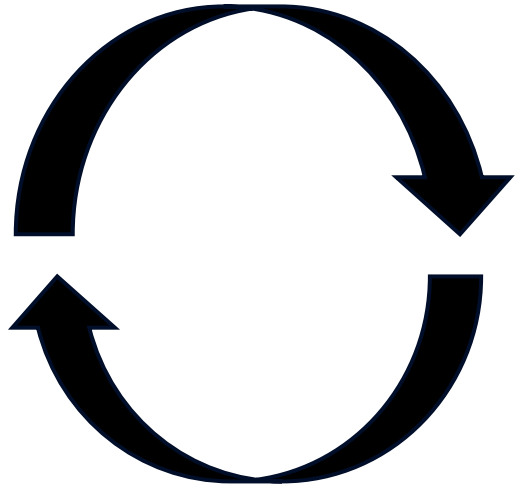
- Uchovanie digitálnych stôp v pôvodnej podobe
- Účelom kontrol integrity je ukázať, že digitálne stopy sa od okamihu ich zaistenia nezmenili
- V praxi proces overovania integrity digitálnych stôp spočíva v porovnaní digitálneho odtlačku (hašu) v čase zaistenia s digitálnym odtlačkom v čase porovnania

7) Objektivita (Objectivity)

- Interpretácia a predkladanie digitálnych stôp by nemali byť zaujaté
- Je veľmi dôležité, aby forenzný analytik odolal predpojatým predstavám a akýmkoľvek tlakom na dosiahnutie konkrétnych záverov
- Najefektívnejším prístupom na dosiahnutie objektivity je nechať čo najviac hovoriť digitálne stopy
- Ďalším efektívnym prístupom k zabezpečeniu objektivity je účasť viacerých nezávislých forenzných analytikov a vzájomné porovnanie výsledkov

8) Opakovateľnosť (Repeatability)

- Dôležité je, aby sa mohli nezávisle overovať zistenia v kontexte forenzného vyšetrovania, keďže sa môže rozhodovať aj o právach osôb
- Je nevyhnutné, aby jeden forenzný analytik zopakoval niektoré alebo všetky analýzy vykonané iným forenzným analytikom



Digitálna forenzná analýza – štandardy

- **ISO/IEC 27035-1:2016** – koncepty a fázy riadenia bezpečnostných incidentov (BI)
- **ISO/IEC 27035-2:2016** – koncept pre plánovanie a prípravu na reakciu na BI
- **ISO/IEC 27035-3:2020** – zodpovednosť zamestnancov a praktické aktivity
- **ISO/IEC 27037:2012** – usmernenia pre konkrétne činnosti pri digitálnych stopách
- **ISO/IEC 27041:2015** – mechanizmy na výber správnych metód
- **ISO/IEC 27042:2015** – analýza a interpretácia digitálnych stôp
- **ISO/IEC 27043:2015** – kľúčové zásady a procesy pri vyšetrovaní BI
- **ISO/IEC 27050** – činnosti v oblasti elektronického zisťovania
- **ISO/IEC 30121:2015** – rámec pre vedenie organizácií pri digitálnom vyšetrovaní
- **RFC 3227** – pokyny pre administrátorov
- **RFC 3161** – mechanizmus na osvedčenie elektronických informácií
- **NIST SP 800-86** – sprievodca integráciou forenzných techník

Priestor na otázky

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť!

Riadenie udalostí a kybernetických bezpečnostných incidentov

Organizačné opatrenia (Blok II)

Kurz: Manažér kybernetickej bezpečnosti vo verejnej správe

Milan Kubina

KC KYB UNIZA, https://kc.uniza.sk/

milan.kubina@fri.uniza.sk