Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Ochrana proti škodlivému kódu a nežiaducemu obsahu

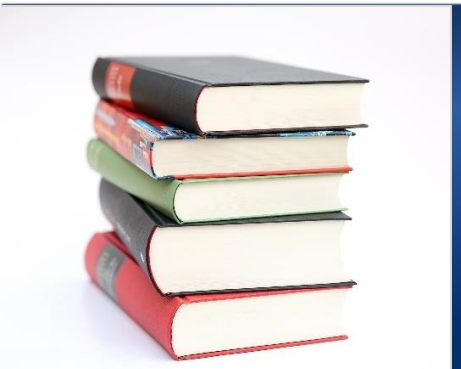
Technické opatrenia (Blok IV)

Kurz: Manažér kybernetickej bezpečnosti

doc. Ing. Gabriel Koman, PhD.

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

gabriel.koman@uniza.sk



Obsah

- Teória, koncepty a metódy systémového inžinierstva
- Zásady určovania bezpečnostne relevantných zdrojov informácií a princípy tvorby prípadov použitia
- Základná architektúra operačných systémov
- Bezpečnostné koncepty v operačných systémoch

Teória, koncepty a metódy systémového inžinierstva

Teória, koncepty a metódy systémového inžinierstva

- **Systémové inžinierstvo (SI):**
  - *Interdisciplinárny prístup a prostriedok na umožnenie realizácie úspešných systémov. Zameriava sa na definovanie zákazníckych potrieb a požadovaných funkcií na začiatku vývoja a pokračuje až po návrh, implementáciu a prevádzku systému*.
  - Ciele:
    - Koordinácia rôznych disciplín pri návrhu a vývoji komplexného systému
    - Zabezpečenie správnosti riešenia -> systém robí to, čo má (validácia)
    - Zabezpečenie kvality riešenia -> systém je zostrojený správne (verifikácia)
    - Minimalizácia rizík (technických, bezpečnostných, ekonomických)
    - Zohľadnenie životného cyklu systému už od jeho návrhu

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

Teória, koncepty a metódy systémového inžinierstva

- **Systémové inžinierstvo (SI) – základné pojmy:**
  - **Systém**
    - Súbor prvkov (ľudia, technológie, procesy), ktoré kooperujú na dosiahnutie spoločného cieľa
  - **Životný cyklus systému (System Life Cycle – SLC)**
    - Zahŕňa fázy: požiadavky, návrh, vývoj, testovanie, prevádzka, údržba, vyradenie
  - **Požiadavky**
    - Jasne definované funkčné a nefunkčné požiadavky na bezpečný systém
  - **Stakeholderi**
    - Osoby alebo organizácie, ktoré majú záujem na systéme, napr. používateľ, správca, vlastník, regulačné orgány a pod.
  - **Integrácia**
    - Prepojenie komponentov do jedného funkčného celku
  - **Verifikácia a validácia**
    - Verifikácia = robíme veci správne
    - Validácia = robíme správne veci

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

Teória, koncepty a metódy systémového inžinierstva

- **Princípy SI:**
  - Komplexný prístup (holistický prístup)
    - Systém je viac než len súčet jeho častí -> kľúčové sú interakcie
  - Iteratívnosť
    - Vývoj systému prebieha v cykloch (napr. špirálový model), nie lineárne.
  - Orientácia na požiadavky
    - Každé rozhodnutie musí byť spojené s požiadavkami stakeholderov.
  - Správa zložitosti
    - Rozdelenie systému na komponenty, modularita, abstrahovanie detailov
  - Riadenie rizík
    - Nepretržité hodnotenie a mitigácia technických aj bezpečnostných rizík
  - Životný cyklus
    - Systém sa navrhuje s ohľadom na celý jeho život -> od návrhu po vyradenie

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

Teória, koncepty a metódy systémového inžinierstva

- **Význam SI v kontexte kybernetickej bezpečnosti (KB)**
  - KB je nevyhnutnou súčasťou návrhu a vývoja systému
  - SI = rámec pre zabudovanie bezpečnosti do každého z krokov životného cyklu vývoja systému
  - Úlohy manažéra KB v SI:
    - Presadzovať bezpečnostné požiadavky pri definovaní systému
    - Koordinovať rôznorodé tímy –> IT, vývojárov, zamestnancov bezpečnosti, prevádzku
    - Riadiť návrh architektúry systému s ohľadom na bezpečnostné domény, segmentáciu, ochranné opatrenia
    - Zapájať sa do verifikačných a validačných procesov s cieľom testovať bezpečnosť navrhovaného systému
  - Roly manažéra KB v SI:
    - Systémová –> spája ľudí, technológie a procesy
    - Bezpečnostná (bezpečnostný architekt) -> rozumie architektúre systému a dokáže identifikovať jeho slabiny
    - Manažérska (CISO) -> vedie zabezpečenie systému ako celku, nie len jednotlivých komponentov
    - Konzultačná (Security Consultant) -> vyhodnocuje dopady rozhodnutí – napr. či zmena softvéru alebo poskytovateľa ovplyvní bezpečnosť systému.

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

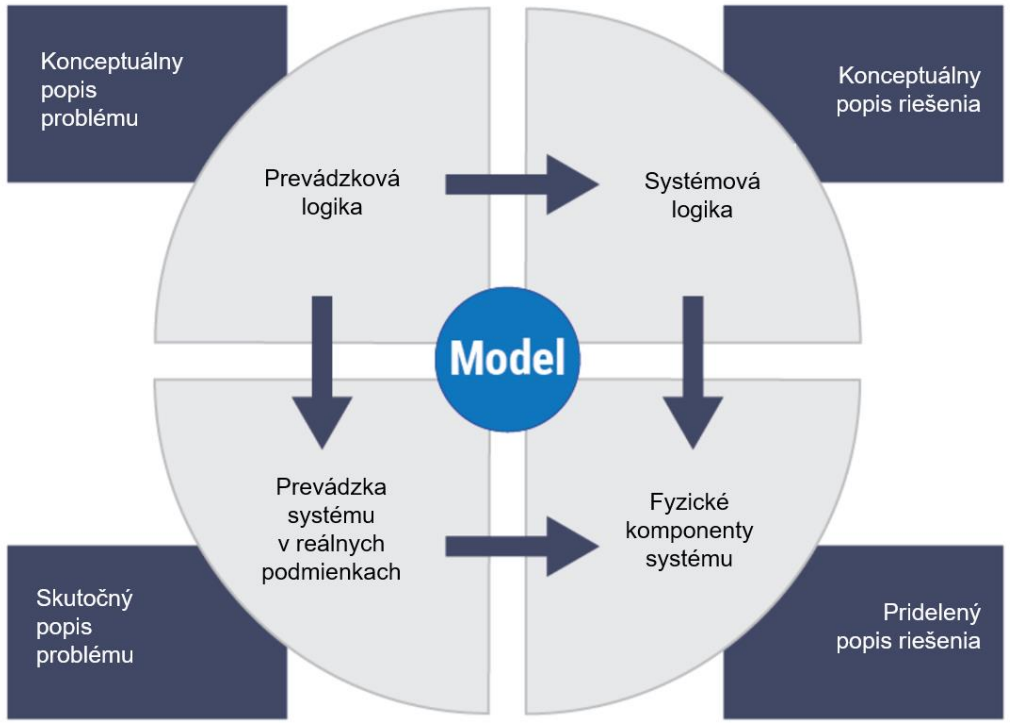
Teória, koncepty a metódy systémového inžinierstva

- **Príklady SI v kontexte kybernetickej bezpečnosti (KB)**
  - 1. **Návrh nemocničného informačného systému**
    - **SI** zabezpečuje koordináciu a kooperáciu:
      - Klinických odborníkov, vývojárov, správu IT, manažment, regulačné orgány atď.
    - **Manažér KB:**
      - Definuje bezpečnostné požiadavky (ochrana údajov pacientov, auditné záznamy)
      - Sleduje integráciu s medicínskymi zariadeniami (IoT)
      - Zabezpečuje súlad so zákonmi (GDPR a ďalšou legislatívou)
  - 2. **Kritická infraštruktúra – SCADA systém**
    - **SI** riadi:
      - Architektúru celej siete, integráciu senzorov, softvérov a operátorov
    - **Manažér KB:**
      - Identifikuje kritické body v architektúre (napr. vstupné brány)
      - Implementuje princíp segmentácie, identifikuje anomálie a pod.
      - Zabezpečuje nepretržité monitorovanie a reakciu na incidenty

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

Metódy systémového inžinierstva

- **Model-Based Systems Engineering (MBSE)**
  - Modelovo riadené systémové inžinierstvo
    - Nahrádza tradičný dokumentačný prístup modelmi
      - Modely reprezentujú požiadavky, architektúru, správanie a overenie systému
  - **Možnosti pre manažéra KB:**
    - Smerovanie bezpečnostných požiadaviek na konkrétne prvky systému
    - Detekcia bezpečnostných slabín v návrhu
    - Podpora analýzy dopadov pri zmene systému
    - Jednotné vizuálne porozumenie medzi tímami (bezpečnosť, vývoj, prevádzka...)
  - Nástroje:
    - SysML, Enterprise Architect, MagicDraw, Cameo Systems Modeler



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

Metódy systémového inžinierstva

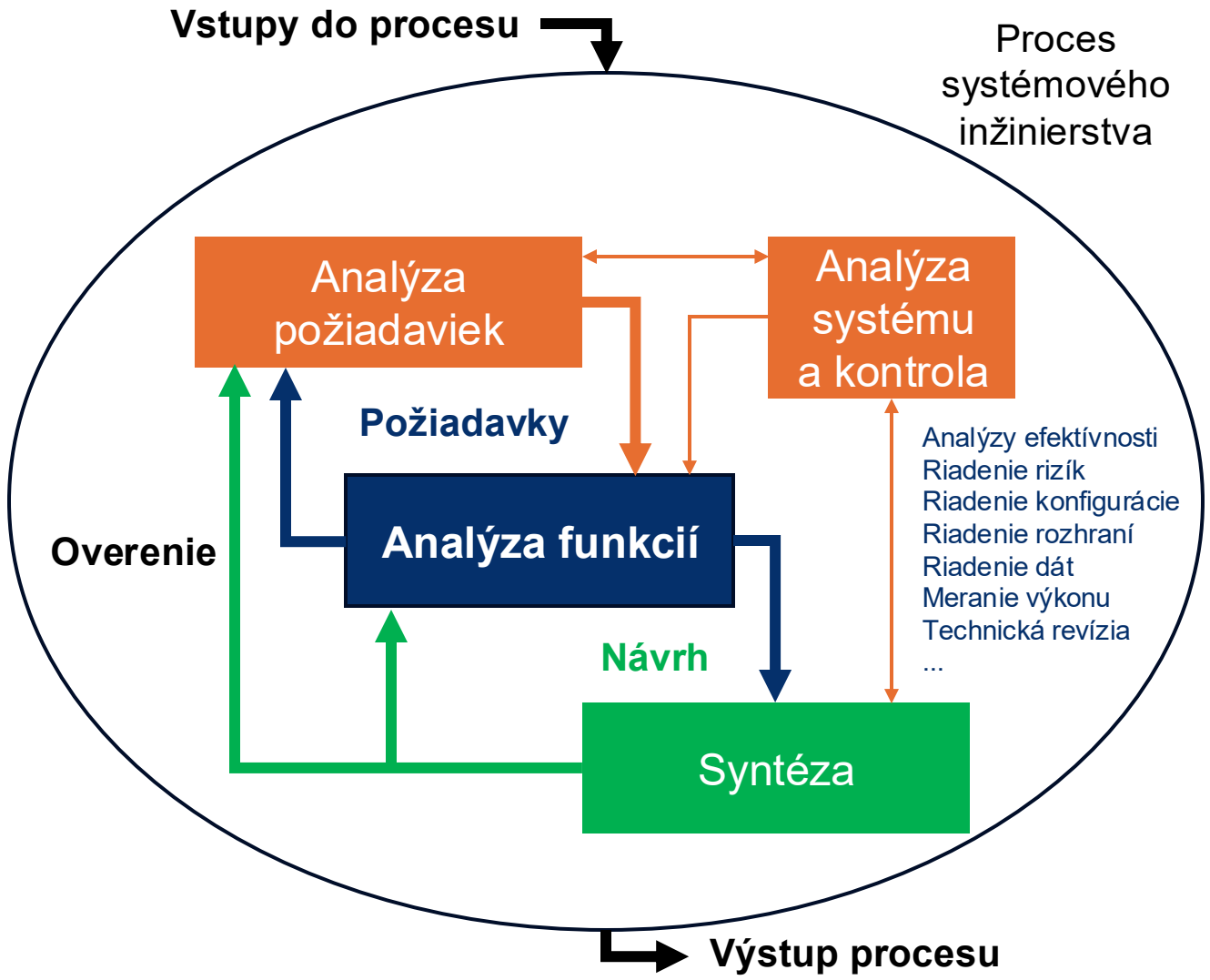
- **Model-Based Systems Engineering (MBSE)**

  - **Príklad:** Návrh bezpečnostnej architektúry nemocničného IS
    - Nemocnica zavádza nový informačný systém, ktorý bude prepájať portál pacientov, laboratórny systém a zdravotnícke IoT zariadenia
    - **Uplatnenie metódy:**
      - Manažér KB vytvára model bezpečnostnej architektúry
        - Definuje prvky napr.: autentifikačná služba, systém logovania, šifrovaný kanál atď.
      - Požitie modelu -> trasovanie požiadaviek:
        - Napr. požiadavka *dáta pacienta musia byť dôverné* sa trasuje na *komunikačné kanály musia byť šifrované*
      - Zmena v jednom module (napr. zmena systému logovania) sa prejaví v modeli
        - Pomáha odhaliť dopady
    - Prínosy:
      - Vizualizácia závislostí v kontexte informačnej bezpečnosti
      - Rýchlejší bezpečnostný audit
      - Jasná komunikácia s architektmi a vývojármi

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

Metódy systémového inžinierstva

- **Analýza funkcií (Functional Analysis)**
  - Rozloženie systému na funkcie a podfunkcie, ktoré je možné analyzovať, špecifikovať a priradiť im zodpovednosti
  - **Možnosti pre manažéra KB:**
    - Identifikácia kritických funkcií z pohľadu bezpečnosti
      - Napr. autentifikácia, šifrovanie, detekcia útokov
    - Definovanie kontrolných bodov v systéme
    - Základ pre návrh security use cases a testovacích scenárov



Metódy systémového inžinierstva

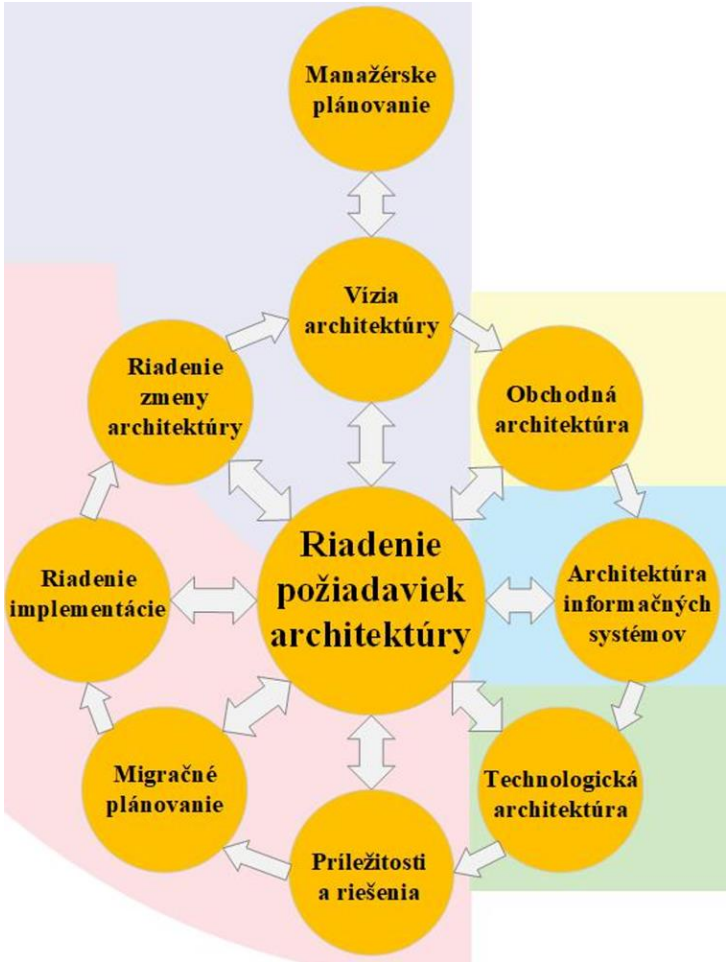
- **Analýza funkcií (Functional Analysis)**

  - **Príklad:** Systém pre prístup do dátového centra
    - Podnik vyvíja systém pre prístup do dátového centra s pomocou kariet, biometrie a vzdialeným monitoring
    - **Uplatnenie metódy:**
      - Manažér KB **identifikuje funkcie** relevantné z hľadiska KB, napr.: autentifikácia osoby, otvorenie dverí, logovanie pokusu o vstup atď.
      - Funkcia *otvorenie dverí* je rozšírená o podmienku: *musí byť splnená viacfaktorová autentifikácia*
      - Na základe funkcií sa určia bezpečnostne kritické body (napr. autorizácia, reakcia na neoprávnený pokus)
    - Prínos:
      - Prehľadné oddelenie funkcií, ktoré musia byť chránené
      - Východisko pre návrh testovacích scenárov
      - Uľahčenie spolupráce s vývojármi a prevádzkou

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

Metódy systémového inžinierstva

- **Návrh architektúry systému (System Architecture Design)**
  - Definovanie štruktúry systému
    - Komponenty, ich rozhrania, vzťahy a spôsoby komunikácie
  - **Možnosti pre manažéra KB:**
    - Návrh segmentácie siete a bezpečnostných zón (napr. DMZ, core, trusted)
    - Princípy least privilege, zero trust, defense-in-depth
    - Zohľadnenie redundancie, dostupnosti, odolnosti
    - Určenie bezpečnostných domén a tokov dát
  - Štandardy a rámce:
    - TOGAF
    - Zachman Framework
    - SABSA (bezpečnostná architektúra)



Metódy systémového inžinierstva

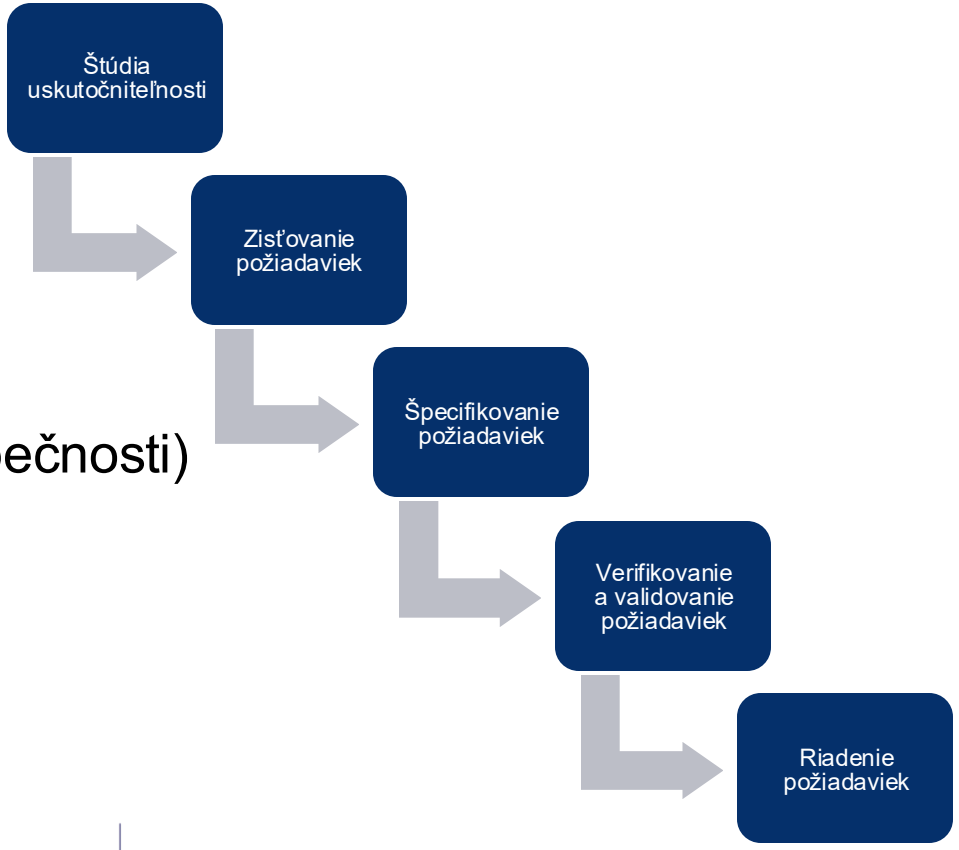
- **Návrh architektúry systému (System Architecture Design)**

  - **Príklad:** Bezpečná architektúra SCADA systému pre energetiku
    - SCADA sieť riadi elektrické rozvody na regionálnej úrovni
    - **Uplatnenie metódy:**
      - Uplatnenie princípu segmentácie siete:
        - Oddelenie podnikovej IT, SCADA siete, DMZ a prístupových bodov
      - Manažér KB navrhuje jednosmerné brány (data diode) medzi segmentmi
      - Definuje toky údajov, ktoré musia byť monitorované:
        - Napr.: prenos z externého prostredia do riadiaceho centra
      - Spolupracuje na mapovaní aktív, rozhraní a rizík každého komponentu
    - Prínos:
      - Obrana *defense-in-depth* už v návrhu
      - Vysoká odolnosť voči laterálnemu pohybu útočníka
      - Prehľadná dokumentácia pre audit

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

Metódy systémového inžinierstva

- **Riadenie požiadaviek (Requirements Engineering)**
  - Proces identifikácie, získavania, analýzy, špecifikácie, validácie a riadenia potrieb a očakávaní zainteresovaných strán pre softvérový systém
  - **Možnosti pre manažéra KB:**
    - Zabezpečenie, že sú všetky požiadavky na bezpečnosť identifikované (napr. dostupnosť, dôvernosť, integrita)
    - Riadenie zmien v zmysle sledovania požiadaviek až na implementačné opatrenia
    - Podpora pri presadzovaní legislatívy a noriem (napr. GDPR, ISO 27001, zákon o kybernetickej bezpečnosti)
  - Nástroje:
    - IBM DOORS, Jama, JIRA + Confluence



Metódy systémového inžinierstva

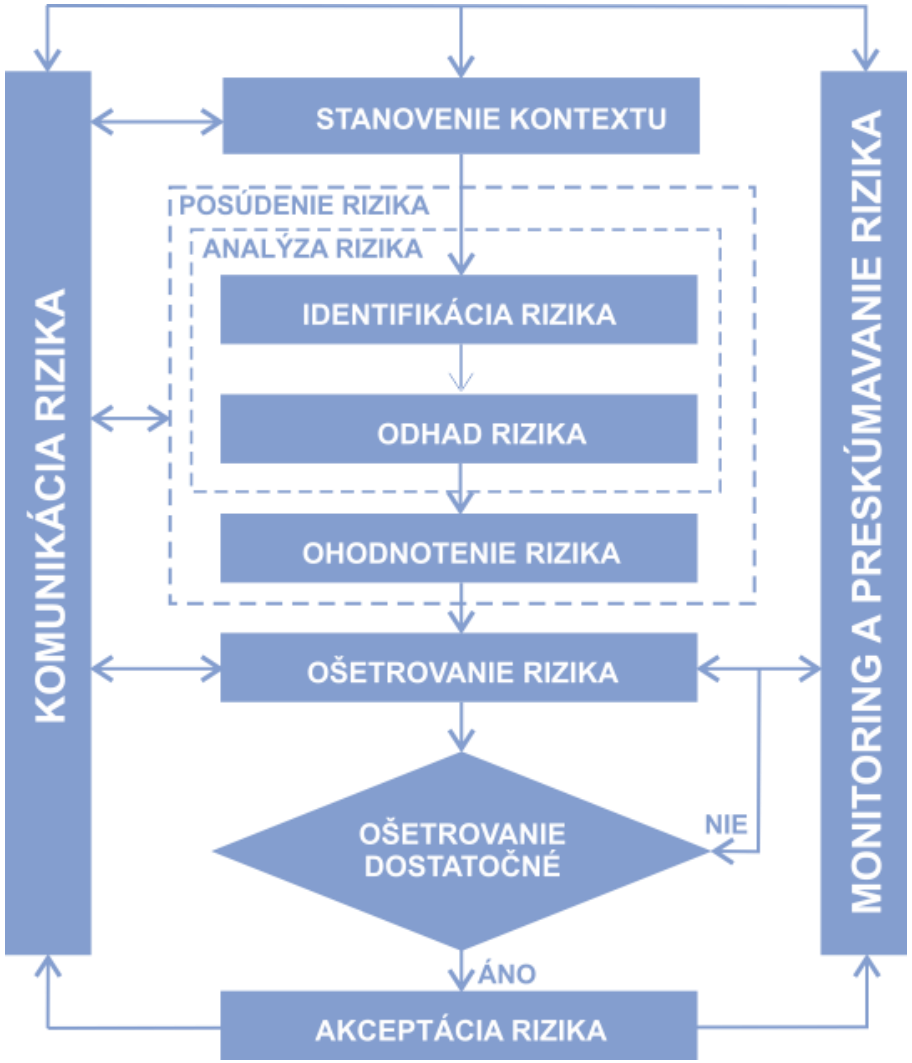
- **Riadenie požiadaviek (Requirements Engineering)**

  - **Príklad:** Vývoj cloudovej aplikácie na spracovanie osobných údajov
    - Podnik vyvíja SaaS aplikáciu, ktorá spracováva citlivé údaje klientov
    - **Uplatnenie metódy:**
      - Manažér KB definuje požiadavky na:
        - šifrovanie, auditovanie, dostupnosť, GDPR a pod.
      - Všetky požiadavky sú evidované v systéme (napr. JIRA) a priradené k implementačným tímom
      - Každú požiadavku má byť možnosť sledovať od zdroja po testovanie
    - Prínos:
      - Prehľad v zodpovednostiach za implementáciu bezpečnostných funkcií
      - Zníženie rizika absencie kritických požiadaviek
      - Podpora pri auditoch a regulácii

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

Metódy systémového inžinierstva

- **Riadenie rizík (Risk Management)**
  - Systematická identifikácia, analýza a ošetrenie rizík, ktoré môžu ohroziť dosiahnutie cieľov systému
  - **Možnosti pre manažéra KB:**
    - Identifikácia hrozieb a zraniteľností už v úvodných fázach projektu
    - Hodnotenie dopadov a pravdepodobností, návrh mitigačných opatrení
    - Zaradenie do širšieho podnikového riadenia rizík (ERM)
    - Prepojenie s bezpečnostnými rámcami ako ISO 27005, NIST RMF, OCTAVE alebo FAIR



Metódy systémového inžinierstva

- **Riadenie rizík (Risk Management)**

  - **Príklad:** Riadenie rizík v projekte migrácie bankového systému na cloud
    - Banka plánuje presun aplikácií z on-premise do cloudu
    - **Uplatnenie metódy:**
      - Manažér KB identifikuje:
        - Aktíva (zákaznícke dáta, API)
        - Hrozby (napr. útoky z iných tenantov)
        - Zraniteľnosti (chyby v konfigurácii)
      - Odhaduje dopad a pravdepodobnosť (podľa ISO 27005)
      - Navrhuje opatrenia: silná segmentácia, šifrovanie, monitorovanie atď.
    - Prínos:
      - Informované rozhodnutia o zabezpečení cloudu
      - Argumentačná báza pre výkonné vedenie
      - Podpora kontinuálneho riadenia a hodnotenia rizík

Metódy systémového inžinierstva

- **Analýza kompromisov (Trade-Off Analysis)**
  - Proces porovnávania, určovania priorít a rozhodovania medzi rôznymi požiadavkami alebo možnosťami návrhu, najmä ak majú zainteresované strany protichodné názory. Zahŕňa použitie techník, ako sú rozhodovacie tabuľky, na uľahčenie vyjednávania a rozhodovania
  - Vyhodnotenie alternatívnych návrhov z hľadiska viacerých kritérií: náklady, výkon, bezpečnosť, udržateľnosť
  - **Možnosti pre manažéra KB:**
    - Porovnanie lokálneho a cloudového riešenia z pohľadu bezpečnosti a nákladov
    - Odhalenie konfliktov medzi bezpečnostnými opatreniami a použiteľnosťou
    - Podpora informovaného rozhodovania
  - Techniky:
    - Pareto analýza
    - Rozhodovacie matice
    - AHP (Analytic Hierarchy Process)

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

Metódy systémového inžinierstva

- **Analýza kompromisov (Trade-Off Analysis)**

  - **Príklad:** Voľba medzi on-premise SIEM a cloudovým SIEM riešením
    - Bezpečnostný tím má rozhodnúť o novej platforme pre logovanie a detekciu incidentov
    - **Uplatnenie metódy:**
      - Manažér KB vytvorí rozhodovaciu maticu s vhodnými kritériami:
        - Napr.: cena, výkon, údržba, legislatíva, bezpečnosť, flexibilita
      - On-premise SIEM má lepšiu kontrolu, ale vyššie náklady
      - Cloud SIEM má nižšie náklady, ale vyžaduje dôveru v poskytovateľa
    - Prínos:
      - Transparentný výber riešenia
      - Možnosť vysvetliť kompromisy vedeniu
      - Minimalizácia neobjektívnych rozhodnutí

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

Metódy systémového inžinierstva

- **Verifikácia a validácia**
  - Procesy zabezpečujúce, že systém robí to, čo má (validácia), a že je vytvorený správne (verifikácia)
    - Vyvíjané softvérové produkty neobsahujú chyby,
    - Sú v súlade s normami kvality
    - Spĺňajú požiadavky zákazníka
  - **Možnosti pre manažéra KB:**
    - Vytváranie testovacích plánov pre zabezpečenie požiadaviek na bezpečnosť
    - Penetračné testovanie, bezpečnostný audit, red teaming
    - Validácia, t. j. že opatrenia na ochranu dát skutočne fungujú

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

Metódy systémového inžinierstva

- **Verifikácia a validácia**

  - **Príklad:** Overenie bezpečnostných opatrení v e-Government portáli
    - Štátna správa zavádza nový elektronický portál pre občanov
    - **Uplatnenie metódy:**
      - Manažér KB definuje testovacie prípady pre: autentifikáciu, logovanie, DDoS ochranu...
      - Prebiehajú penetračné testy a bezpečnostné audity
      - Výsledky sa porovnávajú s požiadavkami na bezpečnosť
    - Prínos:
      - Preukázanie funkčnosti bezpečnostných mechanizmov
      - Identifikácia zlyhaní ešte pred nasadením
      - Akceptovanie regulačných požiadaviek

Teória, koncepty a metódy systémového inžinierstva

- **Životný cyklus systému v kontexte kybernetickej bezpečnosti**

Aplikovanie požiadaviek na bezpečnosť

Aplikovanie princípov bezpečného návrhu (napr. least privilege, defense-in-depth)

Zabezpečený proces vývoja (Secure SDLC)

Penetračné testy, analýza zraniteľností

Monitorovanie, detekcia incidentov

Aktualizácie, revízie, kontinuálne hodnotenie rizík

Bezpečná likvidácia a odstránenie dát

Security Design

- Proces systematického navrhovania bezpečnostných opatrení
  - Cieľ -> predchádzať zraniteľnostiam, ochrana aktív, odolnosť voči hrozbám, minimalizovanie dopadov útokov
- Už vo fáze návrhu
  - Napr.: pri IoT zariadeniach -> funkcia aktualizácie SW
- Odstrániť všetky zadné vrátka, účty a možnosť ladenia
- Pracuje sa s myšlienkou, že útočníci nájdu všetky zakódované zadné vrátka alebo účty a použijú ich na kompromitáciu systému

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

Security Design

- Kontrola vybraných prvkov pri práci s vopred vyrobenými zariadeniami (najmä IoT):
  1. Predvolené heslá
     - Všetky predvolené účty musia byť deaktivované
     - Ak deaktivovanie predvolených účtov nie je možné -> heslá týchto účtov zmeniť na silné heslo
     - Ak je účet pevne zakódovaný (účet ani jeho heslo nie je možné zmeniť) -> zvážiť výber iného zariadenia
  2. Universal Plug and Play (UPnP)
     - Protokol určený na pomoc zariadeniam umiestneným za smerovačom NAT, aby boli automaticky dostupné z internetu
     - Nastavenie automatického sprístupnenia zariadenia na internete = široká škála vektorov útoku
     - UPnP by malo byť na zariadení a na internetovom smerovači vypnuté

Security Design

- Kontrola vybraných prvkov pri práci s vopred vyrobenými zariadeniami (najmä IoT):
  3. Vzdialená správa
     - Niektoré zariadenia využívajú služby vzdialenej správy – napr. Telnet alebo SSH
       - Možnosť monitorovania/odsledovania
       - Všeobecné odporúčanie -> zakázať služby vzdialenej správy pre zariadenia, ku ktorým je možné pristupovať cez internet
       - V rámci siete LAN -> možno použiť šifrovanú službu správy, napríklad SSH
       - Telnet -> riziko -> nešifruje prevádzku a mal by byť zakázaný v každej situácii

  4. Aktualizácie a opravy softvéru
     - Zariadenia a použité technológie -> nutnosť pravidelných aktualizácií
     - Zariadenia a použité technológie -> používať vždy najnovší softvér
     - Ak sa softvér zariadenia nedá aktualizovať -> zvážiť zariadenie nepoužívať / nahradiť iným

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

Security Design

- Kontrola vybraných prvkov pri práci s vopred vyrobenými zariadeniami (najmä IoT):
  5. Šifrovaná komunikácia a certifikáty
     - Mnohé hotové zariadenia (najmä IoT) -> nepodporujú pokročilé bezpečnostné funkcie:
       - Šifrovanie alebo používanie certifikátov
     - Ak zariadenie podporuje takéto pokročilé bezpečnostné funkcie je potrebné ich povoliť a používať

  6. Fyzická bezpečnosť
     - Dôrazne sa odporúča zabezpečiť fyzické miesto nasadenia

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

Zásady určovania bezpečnostne relevantných zdrojov informácií a princípy tvorby prípadov použitia

Ochrana proti škodlivému kódu a nežiadúcemu obsahu

Zásady určovania bezpečnostne relevantných zdrojov informácií a princípy tvorby prípadov použitia

- Bezpečnostne relevantné zdroje informácií:
  - Všetky interné a externé zdroje dát, ktoré môžu ovplyvniť rozhodovanie v oblasti kybernetickej bezpečnosti:
    - Detekciu incidentov
    - Hodnotenie rizík
    - Tvorbu bezpečnostných politík atď.
  - **Zásady určovania bezpečnostne relevantných zdrojov informácií:**
    1. Relevancia vo vzťahu k hrozbám a zraniteľnostiam
    2. Aktuálnosť a spoľahlivosť
    3. Dôveryhodnosť a overiteľnosť zdroja
    4. Zrozumiteľnosť a formát
    5. Možnosť automatického spracovania
    6. Právne a regulačné požiadavky

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

Ochrana proti škodlivému kódu a nežiadúcemu obsahu

Zásady určovania bezpečnostne relevantných zdrojov informácií a princípy tvorby prípadov použitia

1. **Relevancia vo vzťahu k hrozbám a zraniteľnostiam**
   - Priamy, príp. nepriamy vzťah s aktuálnymi alebo potenciálnymi hrozbami
     - Napr. zraniteľnosti, malware, phishing a pod.
     - Príklady:
       - CVE databáza, MITRE ATT&CK, NVD (National Vulnerability Database)
2. **Aktuálnosť a spoľahlivosť**
   - Informácie musia byť aktuálne, verifikované a z dôveryhodných zdrojov
     - Príklady dôveryhodných zdrojov: ENISA, NIST, CERT, ISACA, SANS Institute
3. **Dôveryhodnosť a overiteľnosť zdroja**
   - Preferovanie oficiálnych vedeckých alebo komunitou verifikovaných zdrojov
     - Vedecké databázy: IEEE Xplore, Springer, ScienceDirect atď.

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

Zásady určovania bezpečnostne relevantných zdrojov informácií a princípy tvorby prípadov použitia

4. **Zrozumiteľnosť a formát**
   - Informácie musia byť prezentované tak, aby boli zrozumiteľné pre analytikov, aj manažérov (napr. executive summary vs. technická správa)
5. **Možnosť automatického spracovania**
   - Výhodou sú zdroje, ktoré poskytujú API, RSS feedy, STIX/TAXII formáty pre Threat Intelligence platformy
6. **Právne a regulačné požiadavky**
   - Zdroje musia pokrývať aj informácie o súlade s normami a legislatívou
     - GDPR
     - NIS2
     - ISO/IEC 27001
     - atď.

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

Kategórie zdrojov informácií pre manažéra KB

- **Threat Intelligence**
  - Význam -> proaktívne rozpoznanie hrozieb
  - Príklad: MISP, Anomali, IBM X-Force, VirusTotal
- **Interné logy a SIEM**
  - Význam -> detekcia anomálií a incidentov
  - Príklad: Syslog, Windows eventy, Splunk, QRadar
- **Legislatíva a štandardy**
  - Význam -> súlad, zodpovednosť a reporting
  - Príklady: NIS2, GDPR, ISO/IEC 27001, TISAX
- **Vedecké a výskumné zdroje**
  - Význam -> Strategické plánovanie a rozhodovanie
  - Príklad: IEEE, ScienceDirect, ENISA štúdie
- **Komunitné zdroje**
  - Význam -> Kontext hrozieb a reálne prípady
  - Príklad: CERT, CSIRT, komunitné fóra (Reddit, GitHub)

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

Ochrana proti škodlivému kódu a nežiadúcemu obsahu

Zásady určovania bezpečnostne relevantných zdrojov informácií a princípy tvorby prípadov použitia

- **Nástroje umelej inteligencie v kontexte kybernetickej bezpečnosti**
  - Nepredstavujú priamo zdroje informácií, ale nástroje na prácu s nimi
  - Použiteľnosť závisí od:
    - Dát, ktoré spracúvajú
    - Kontextu, ktorý dostanú od používateľa
    - Typu vstupných zdrojov (web, interné dokumenty, knowledge base, API atď.)

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

Zásady určovania bezpečnostne relevantných zdrojov informácií pri práci s AI nástrojmi

1. Overenie pôvodu dát

- AI nástroje generujú výstupy na základe tréningových alebo online dát
- Je potrebné overovať:
  - Cituje AI zdroje?
  - Je výstup založený na dôveryhodných autoritách (NIST, ENISA, MITRE)?

2. Kontext a účel použitia

- Manažér KB musí definovať:
  - Účel využitia AI – napr. sumarizácia správy / návrh bezpečnostnej stratégie
  - Čo má AI ignorovať – napr. výstupy bez overených zdrojov alebo generické odpovede

3. Kritické myslenie a dôsledná kontrola faktov

- AI môže generovať presvedčivé ale nesprávne odpovede -> *“halucinuje“*
  - Z toho dôvodu je potrebné overovať AI výstupy s dôveryhodnými zdrojmi
  - Príklad: ak AI cituje normu ISO 27001, manažér by mal mať prístup k jej plnému zneniu pre overenie výstupu AI

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

Zásady určovania bezpečnostne relevantných zdrojov informácií pri práci s AI nástrojmi

4. Právne a etické hľadiská

- Zverejňovanie citlivých údajov AI nástroju môže byť v rozpore s internou politikou organizácie alebo GDPR
  - Z toho dôvodu je vhodné používať AI len na neklasifikované alebo anonymizované údaje
  - Nástroje ako napr.: Microsoft Security Copilot riešia túto požiadavku pomocou privátnej AI infraštruktúry

5. Aktuálnosť a relevantnosť

- AI musí pracovať s aktuálnymi hrozbami
  - Napr.: Gemini a Perplexity AI majú prístup k zdrojom internetu a sú vhodné na monitoring trendov

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

Zásady určovania bezpečnostne relevantných zdrojov informácií pri práci s AI nástrojmi

- **Pozícia AI v rámci bezpečnostne relevantných zdrojov informácií**
  - AI nástroje nie sú zdroje informácií samé o sebe
    - Urýchľujú a zvyšujú efektívnosť spracovania už existujúcich informácií
    - AI nevytvára nové informácie, ale dokáže spracovať, analyzovať a interpretovať existujúce dáta rýchlejšie a presnejšie než tradičné metódy
    - Príklad: V oblasti kybernetickej bezpečnosti môže **AI** analyzovať miliardy záznamov o sieťovej prevádzke, identifikovať vzory a anomálie, ktoré naznačujú potenciálny útok. **Človek**, analytik by možno strávil dni alebo týždne vykonávaním podobnej úlohy, ale AI nástroje túto úlohu vykonajú v reálnom čase, čím urýchlia reakčný čas na hrozby a poskytnú presnejšie výsledky.
  - Pri požívaní AI nástrojov **by mal manažér KB zabezpečiť:**
    - Validáciu výstupov z AI cez oficiálne zdroje
      - NIST, ISO, ENISA...
    - Kontrolu zdieľania dát smerom do AI
    - Vytvorenie interných pravidiel pre používanie AI (napr. AI Use Policy)
    - Využívanie AI na prípadné zefektívnenie rozhodovania a auditu

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

Ochrana proti škodlivému kódu a nežiadúcemu obsahu

Zásady určovania bezpečnostne relevantných zdrojov informácií a princípy tvorby prípadov použitia

- **Prehľad vybraných AI nástrojov**

Nástroj	Poskytovateľ	Charakteristika a využitie pre manažéra KB
ChatGPT	OpenAI	Generovanie textu, analýza logov, navrhovanie politík, threat modeling
Gemini	Google (DeepMind)	Prepojenie s vyhľadávaním Google, výskum, sumarizácia hrozieb a trendov
Claude	Anthropic	Kontextovo dlhé dokumenty, etické odporúčania, simulácia scenárov
Copilot	Microsoft	Integrácia do MS365, podpora pre IT správu, generovanie dokumentácie, bezpečnostná analýza
Perplexity AI	Perplexity.ai	Vyhľadávanie s citáciami, relevantné najmä pri OSINT, hrozbách a výskume

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

Princípy tvorby prípadov použitia (Use Case)

- **Use case** v oblasti kybernetickej bezpečnosti opisuje konkrétny scenár hrozby alebo bezpečnostnej udalosti, na ktorý má systém alebo tím reagovať
  - Využíva sa napr. v SIEM systémoch, SOAR riešeniach a pri tvorbe bezpečnostných politík.
- **Princípy:**
  1. Zameranie na riziko
     - Každý use case musí byť odvodený z analýzy rizík alebo modelovaných hrozieb (napr. STRIDE, DREAD, PASTA).
  2. Prehľadná štruktúra
     - Prvky use case:
       - Názov
       - Popis hrozby/scenára
       - Zdroje informácií
       - Detekčné pravidlá
       - Reakčné opatrenia
       - Metriky efektivity (napr. MTTR)

Princípy tvorby prípadov použitia (Use Case)

- **Princípy:**
  3. Mapovanie na frameworky
     - Use cases by mali byť naviazané na známe štandardy napr.:
       - MITRE ATT&CK
       - ISO/IEC 27035
       - COBIT
       - NIST CSF
  4. Testovateľnosť a merateľnosť
     - Možnosť testovania v kontrolovanom prostredí
       - Napr.: pomocou red teaming, purple teaming, simulácií s nástrojmi ako Caldera a pod.
  5. Lifecycle manažment
     - Use case nie je statický
       - Potreba pravidelne revidovať, upravovať na základe incidentov a nových hrozieb

Princípy tvorby prípadov použitia (Use Case)

- **Životný cyklus implementácie prípadov použitia**
  1. **Identifikácia rizika/hrozby**
     - Na základe informácií risk assessmentu alebo threat intelligence
     - Rola manažéra KB:
       - Určiť priority na základe biznis dopadov
  2. **Návrh Use Case**
     - Vytvorenie a špecifikácia Use Case
     - Rola manažéra KB:
       - Potvrdiť súlad s obchodnými cieľmi a použitú metriku
  3. **Implementácia**
     - Technická konfigurácia pravidiel, upozornení, automatizácie atď.
     - Rola manažéra KB:
       - Pridelenie zodpovedností
       - Kontrolovanie progresu

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

Princípy tvorby prípadov použitia (Use Case)

- **Životný cyklus implementácie prípadov použitia**
  4. **Testovanie**
     - Simulácie (napr. Purple Team, Red Team, Atomic Red Team)
     - Rola manažéra KB:
       - Rozhodnutie o spôsobe a rozsahu testovania
  5. **Úprava a optimalizácia**
     - Úpravy podľa výsledkov testov a incidentov
     - Rola manažéra KB:
       - Sledovať spätnú väzbu a presadzovať úpravy
  6. **Prevádzka a monitorovanie**
     - Rutinná prevádzka a sledovanie Use Case
     - Rola manažéra KB:
       - Zabezpečenie vhodného spôsobu reportovania informácií pre vedenie
  7. **Revízia**
     - Pravidelné aktualizácie Use Case podľa zmien na základe hrozieb
     - Rola manažéra KB:
       - Riadenie kontinuálne zlepšovania / cyklu (napr. podľa PDCA, ISO 27001 a pod.)

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

Princípy tvorby prípadov použitia (Use Case)

- **Otázky v súvislosti so životným cyklom implementácie prípadov použitia**
  - **Manažér KB:**
    - Je Use Case zameraný na riziko, ktoré ohrozuje stanovené ciele?
    - Je k dispozícii dostatok zdrojov na implementáciu?
      - Ľudské
      - Technické
      - Finančné
    - Aké metriky preukážu, že Use Case funguje správne?
    - Je Use Case v súlade s politikami a normami?
      - NIS2
      - ISO/IEC 27001
    - Ako bude Use Case ovplyvňovať používateľské prostredie?
      - False positives
      - UX

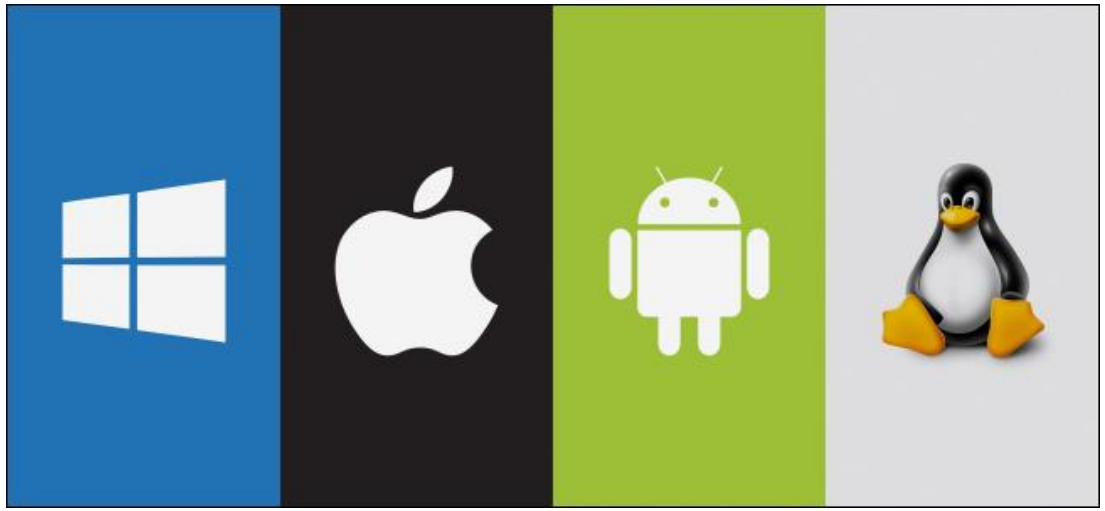
Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

Základná architektúra operačných systémov

doc. Ing. Jozef Kostolný, PhD.

Čo je to operačný systém?

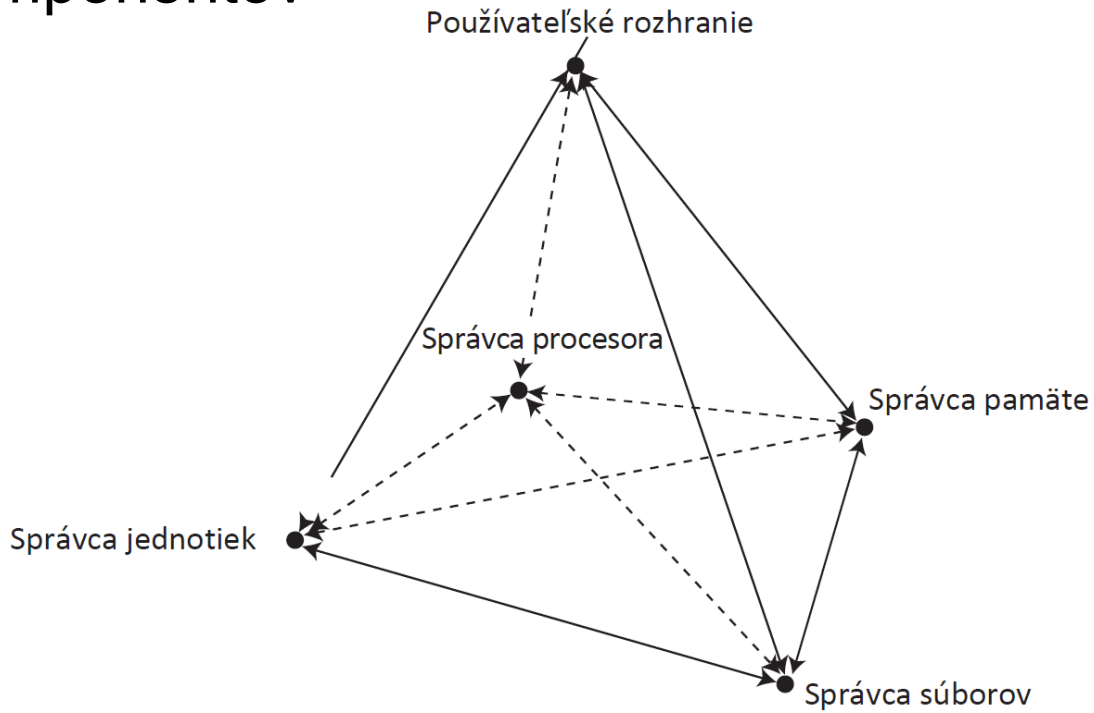
- pochopenie OS znamená chápanie fungovania celého počítačového systému
- OS je riadiaci softvér, ktorý manažuje dostupný hardvér aj softvér
  - správa každého súboru, jednotky, pamäte, akýkoľvek čas procesora



- Čo od neho požadujeme?
  - prijatie odoslaného príkazu
  - spätnú väzbu, či je príkaz prijatý a vykonávaný alebo došlo k chybe

OS ako softvér

- jednoduchá reprezentácia spolupráce komponentov



- základom každého OS:
- Správca procesora
- Správca pamäte
- Správca jednotiek
- Správca súborov

- používateľské rozhranie dovoľuje ich obsluhovať

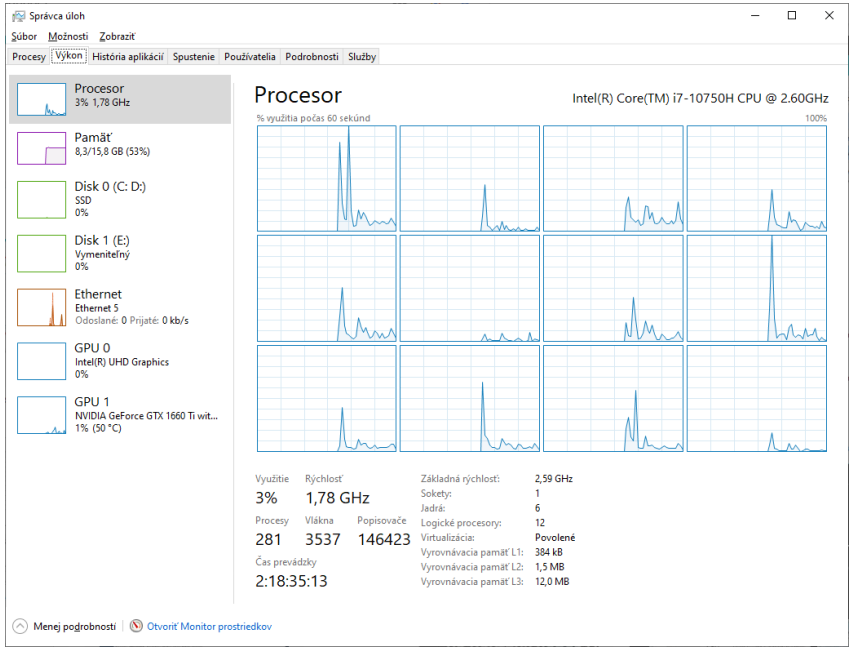
Základné úlohy OS

- aby systém fungoval hladko musí každý manažér minimálne zabezpečovať:
- monitorovanie systémových zdrojov
- presadzovanie politiky priradzovania zdrojov jednotlivým komponentom
- aký zdroj, kedy a koľko
- prideľovať zdroje podľa potreby
- odoberať zdroje podľa potreby

- Príklad:
- Správca pamäte musí sledovať stav voľnej pamäte počítača, musí vedieť alokovať správnu veľkosť pamäte pre prichádzajúce procesy a uvoľniť pamäť pre procesy ktoré už pamäť nepotrebujú – všetko riadené politikou aktuálneho typu OS.

Správca procesora

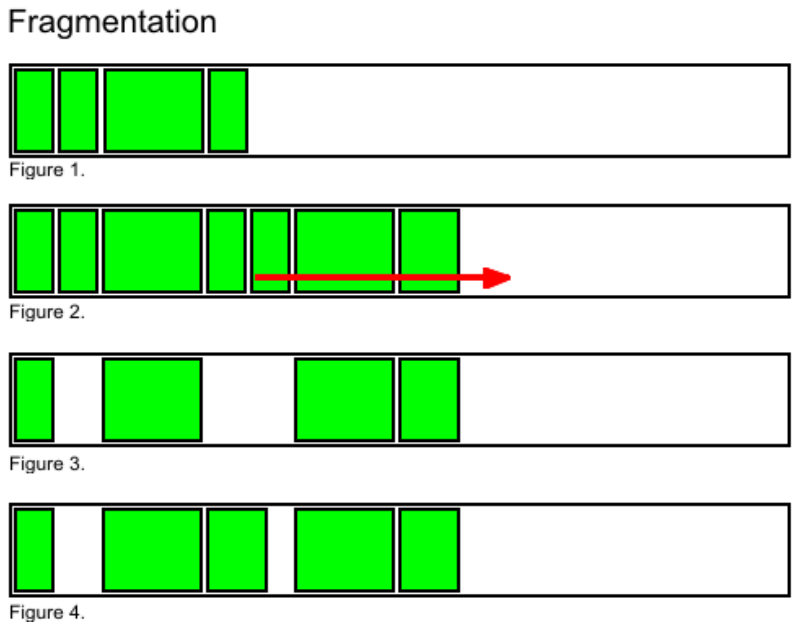
- rozhoduje ako prideliť čas hlavného procesora CPU (central processing unit)
- sledovanie stavu každej úlohy, procesu, vlákna



- efektívny systém máva CPU stále vyťažený
- sleduje a obsluhuje procesy v priebehu spracovania
- zaraďuje nové procesy z frontu do CPU
- odoberá dokončené procesy z CPU

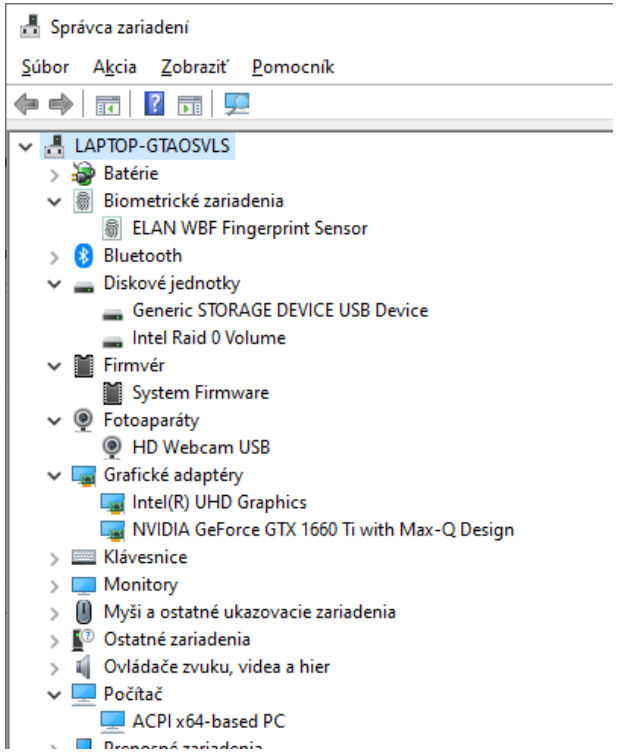
Správca pamäte

- správca hlavnej pamäte počítača – RAM (*Random Access Memory*)
  - validácia požiadaviek na pridelenie priestoru
  - alokovanie voľného priestoru v pamäti pre požiadavku
  - správa voľného priestoru – prípadná fragmentácia
  - uvoľnenie priradeného priestoru
- RAM
  - závislá na elektrickej energii pre zachovanie údajov
  - pri prerušení energie sa údaje vymažú
- ROM (*Read-Only Memory*)
  - energeticky nezávislá pamäť
  - obsahuje firmvér – inštrukcie pre zavedenie OS



Správca jednotiek

- zodpovedný za spojenie s akýmkoľvek zariadením/jednotkou, ktorá je dostupná v systéme
  - tlačiareň, port, disková jednotka
- každé zariadenie má svoj softvér na obsluhu – ovládač zariadenia
  - obsahuje detailné inštrukcie pre OS pre:
    - zapnutie jednotky
    - alokovaniu úlohy na jednotke
    - správne používanie jednotky
    - dealokovanie jednotky keď sa nepoužíva



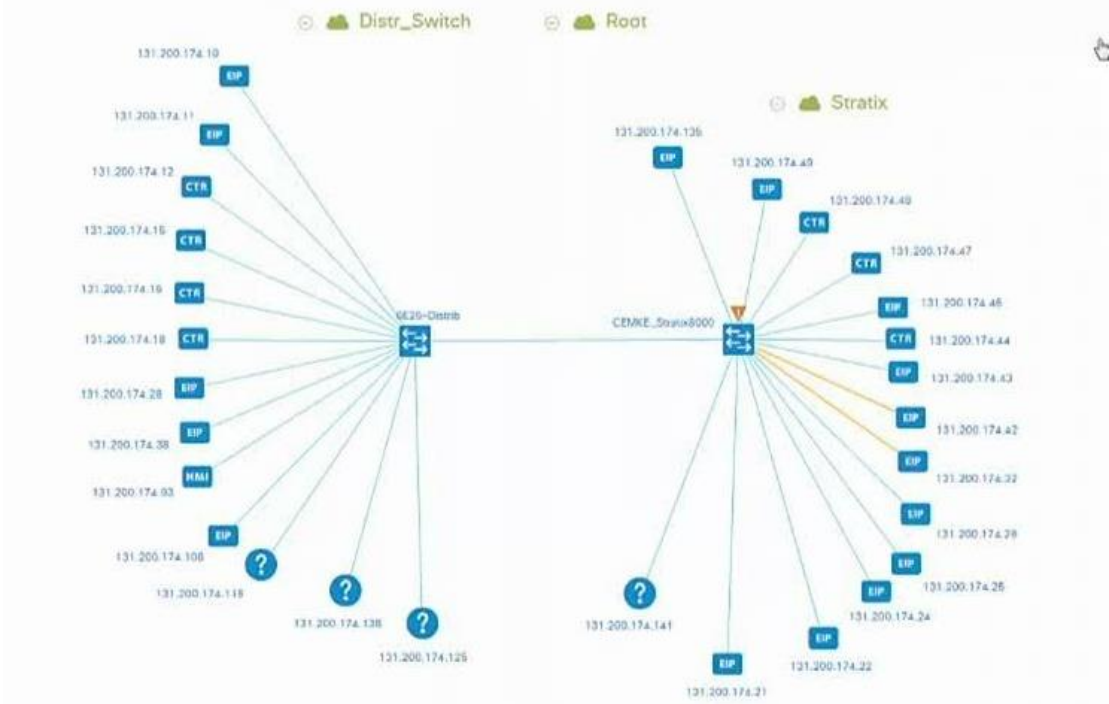
Správca súborov

- sleduje každý súbor v systéme
  - dátové súbory, programové súbory, utility, kompilátory, aplikácie
- rozhoduje kto má k akému súboru prístup
  - podľa aplikácie prístupovej politiky OS – správca, používateľ

- alokovanie voľného miesta na sekundárnej ukladacej jednotke
  - HDD, flash pamäť, archivačné zariadenia ...

Správca siete

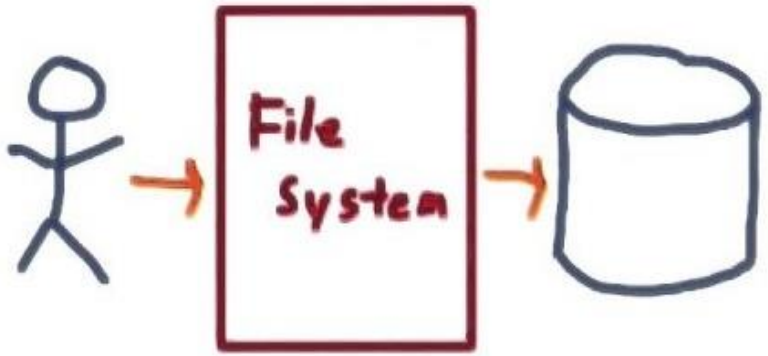
- nemusí byť vždy súčasťou OS
- zodpovedný za pripojenie systému do siete a komunikáciu v nej
  - Internet
  - privátna sieť
- na spojenie sú vyžadované prostriedky v:
  - RAM
  - CPU
  - HDD
  - súbory



Čo je to súborový systém?

- softvér zodpovedný za vytváranie, mazanie, úpravu a riadenie prístupu k súborom a riadenie zdrojov pre súbory

- poskytuje podporu pre spoluprácu so správcom jednotiek
  - podpora vo forme knižníc, programov, údajov

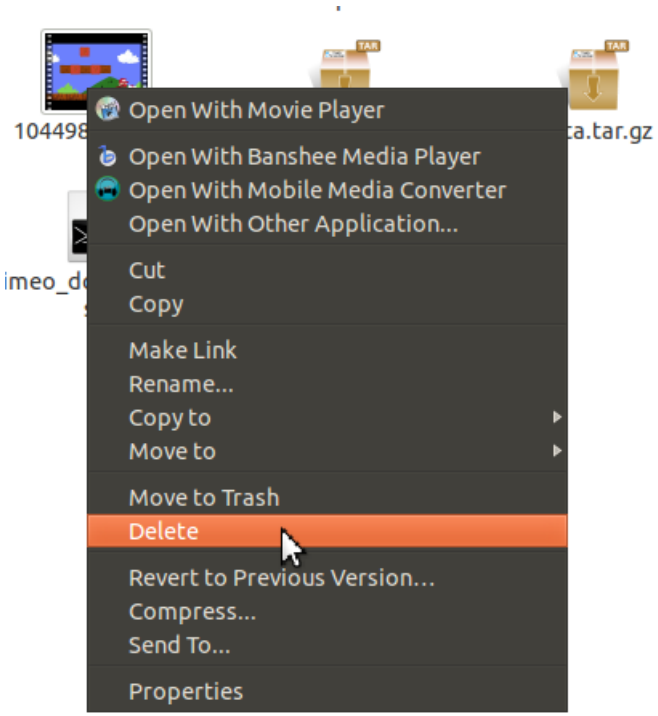


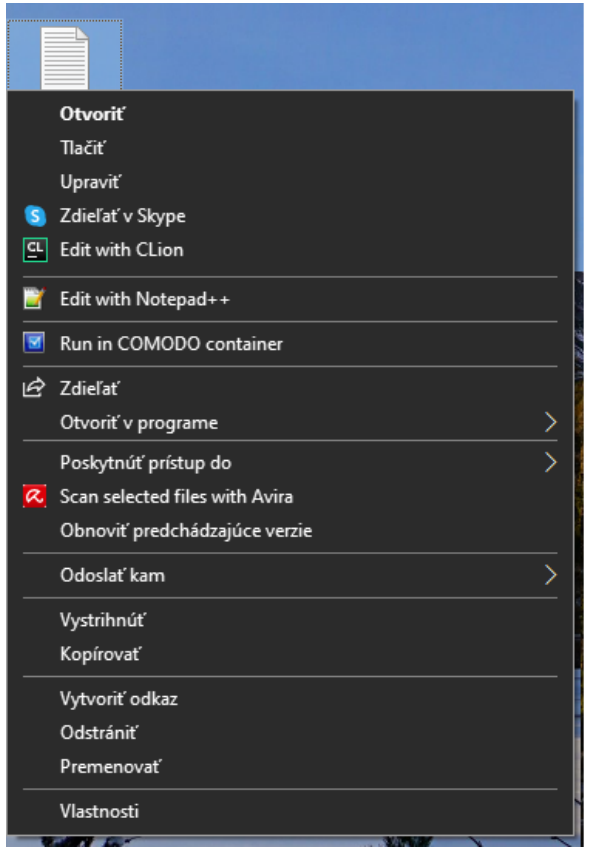
Súborový systém - základné úlohy

1. Uchováva sledovanie kde je každý súbor uložený
2. Určuje politiku, ktorou definuje ako bude súbor uložený, pričom zabezpečuje efektívne využitie priestoru pre ukladanie a zachováva jednoduchý prístup k nim
3. Sprístupňuje každý súbor, na ktorý má používateľ právo prístupu, a sleduje jeho zmeny pri používaní
4. Zakáže prístup pokiaľ je súbor nepoužívaný, oznamuje jeho dostupnosť na otvorenie a priradí ďalšiemu čakajúcemu

Interakcia súborového systému

- odpovedá na špecifické príkazy predefinovanými akciami
- najčastejšie príkazy:
  - Otvor
  - Vymaž
  - Premenuj
  - Kopíruj





Kontrola prístupu

- zdieľanie prístupu – uchovanie integrity údajov
- Úrovne prístupu:
  - **čítanie** - READ
  - **zápis** - WRITE
  - **vykonanie** - EXECUTE
  - **mazanie** – DELETE

- Tabuľka riadenia prístupov

	User 1	User 2	User 3	User 4	User 5
File 1	RWED	R–E–	----	RWE–	--E–
File 2	----	R–E–	R–E–	--E–	----
File 3	----	RWED	----	--E–	----
File 4	R–E–	----	----	----	RWED
File 5	----	----	----	----	RWED

(R = Read Access, W = Write Access, E = Execute Access, D = Delete Access, and a dash (-) = Access Not Allowed)

Bezpečnostné koncepty v operačných systémoch

Ochrana proti škodlivému kódu a nežiaducemu obsahu

Večná otázka

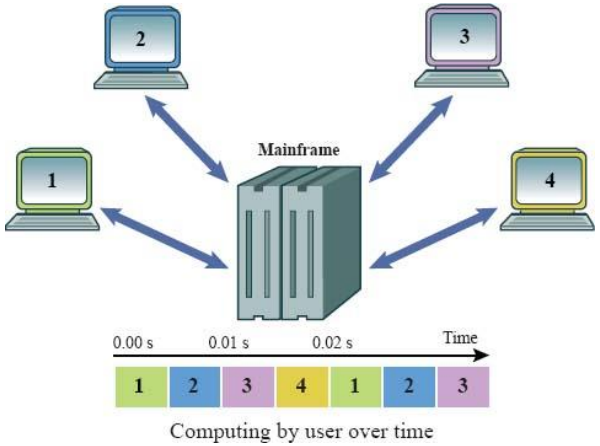
- každý počítačový systém rieši nasledujúci konflikt:
  - zdieľanie prostriedkov
  - chránenie prostriedkov

- riešenie:
  - v minulosti – fyzická ochrana: systém má heslo pre autorizáciu používateľa
  - dnes:
    - dátová komunikácia, zdieľanie cez internet, telekomunikačný softvér, webové stránky, milióny ľudí s prístupom - omnoho zložitejšia situácia
    - mení sa rýchlosťou svetla ... nové technológie, spôsoby útokov....

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

Počet používateľov

- jednotlivec vs. skupina používateľov
- rozdelenie:
  - jednopoužívateľský systém
    - jeden používateľ má prístup k zdrojom systému v jednom čase
  - viacpoužívateľský systém
    - umožňuje prístup viacerým používateľom súčasne pristúpiť ku zdrojom jedného stroja

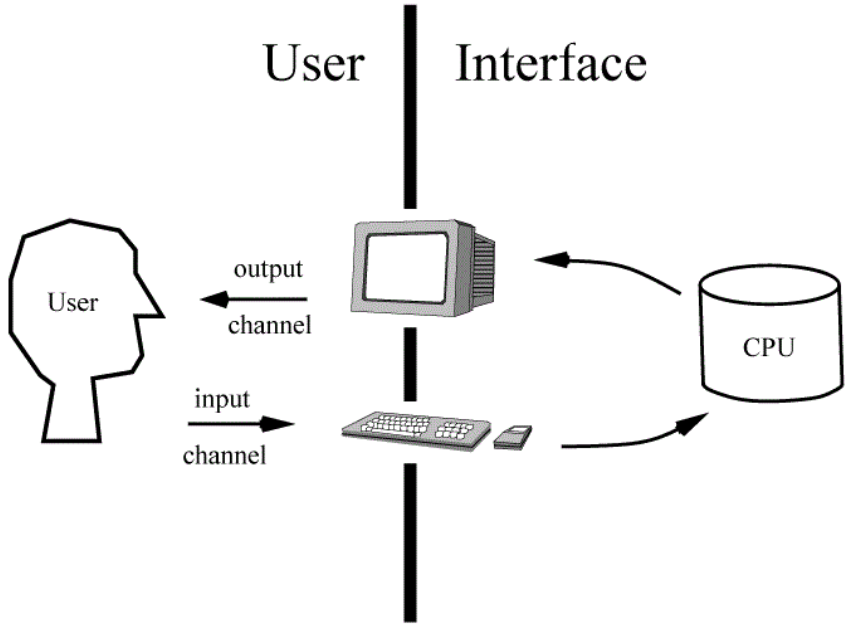


Computing by user over time

Jednopoužívateľský systém

- právo prístupu má práve jeden používateľ v jednom čase
  - zariadenia: mobil, notebook*

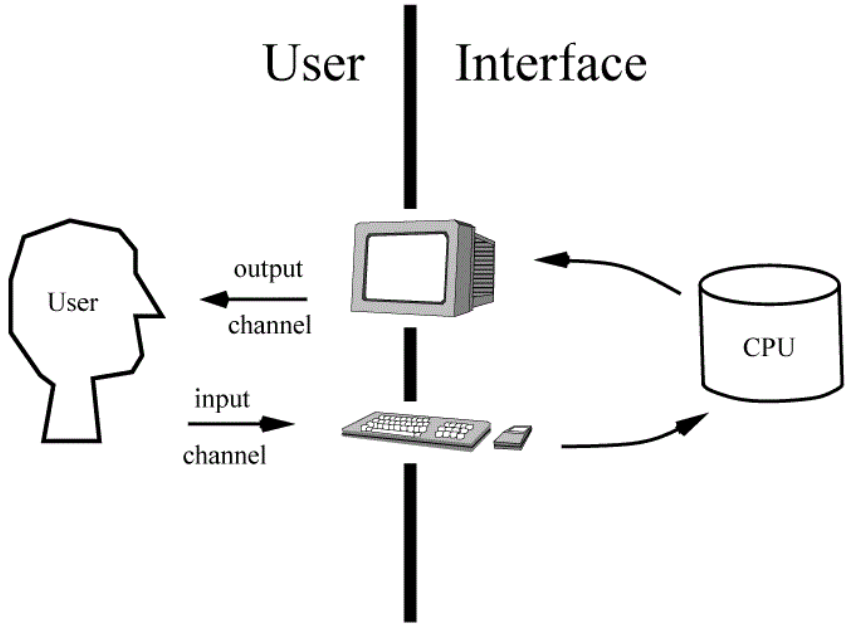
- rozdelenie:
  - jeden používateľ s maximálne jednou úlohou
    - PalmOS, MS-DOS, 86-DOS od IBM
  - jeden používateľ s viacerými úlohami naraz
    - Windows, MacOS



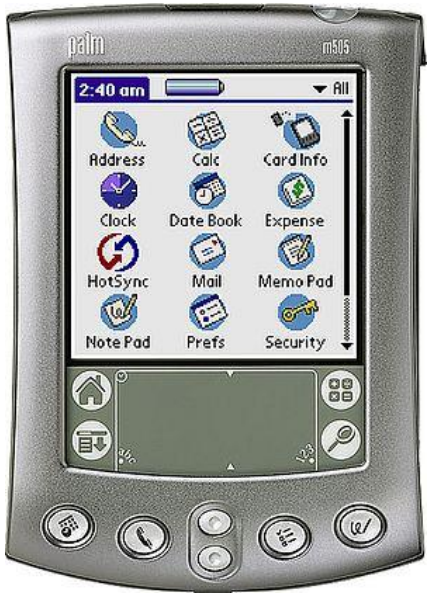
Jednopoužívateľský systém

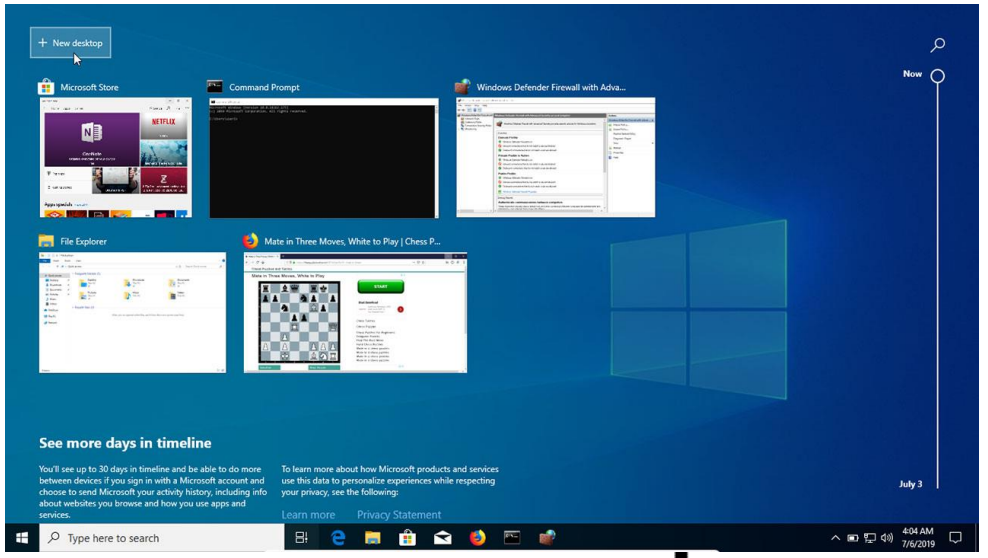
- právo prístupu má práve jeden používateľ v jednom čase
  - zariadenia: mobil, notebook*

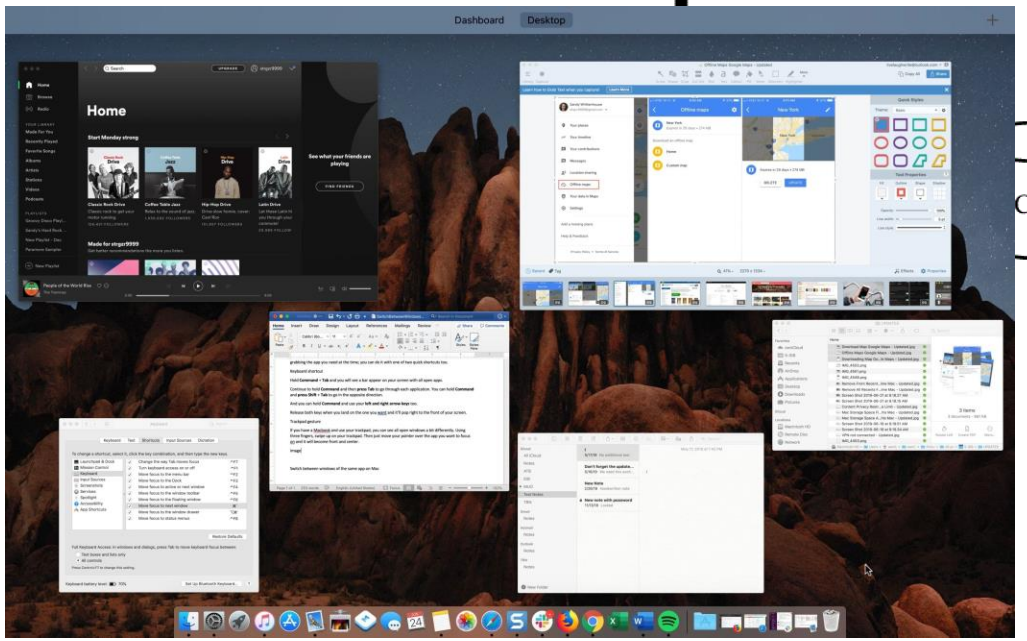
- rozdelenie:
  - jeden používateľ s maximálne jednou úlohou
    - PalmOS, MS-DOS, 86-DOS od IBM
  - jeden používateľ s viacerými úlohami naraz
    - Windows, MacOS



Jednopoužívateľský systém

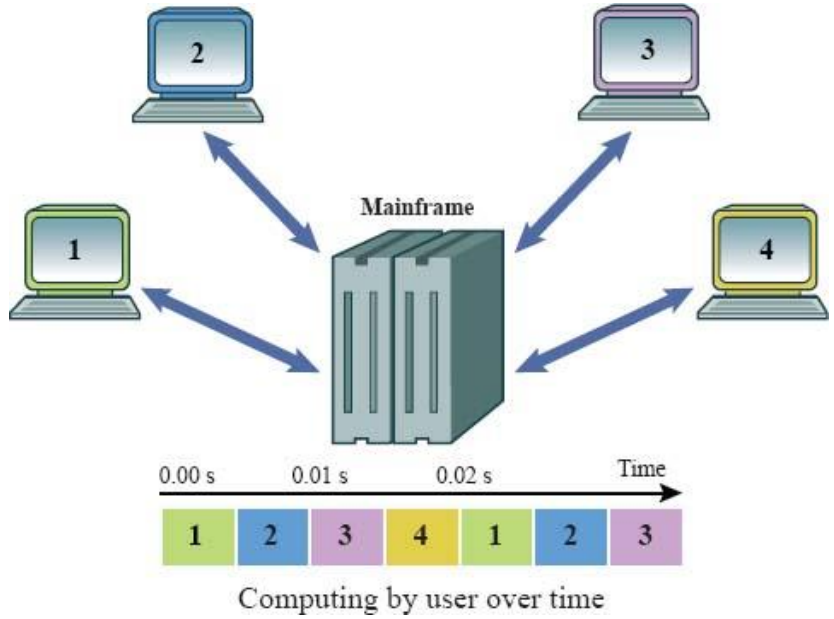






Viacpoužívateľský systém

- prístup má viacero používateľov v jednom čase
  - systémy UNIX, Linux, Windows 10 Azure (Windows Virtual Desktop)
  - pôvodne určený ako systém so zdieľaním času
    - napr. 2 mikrosekundy
  - úlohy ostatných používateľov sa neovplyvňujú
  - prístup k OS je možný aj z rôznych lokácií
  - prístup k serveru



Computing by user over time

Úloha OS v bezpečnosti

- OS má prístup ku všetkým komponentom systému
- zraniteľnosť na akejkoľvek úrovni sprístupňuje systém na útok

- správcovia systémov musia byť preto ostražitý
  - vyzbrojenie OS pre všetky možné útoky aby sa zabránilo zlyhaniu

Odolnosť systému

- schopnosť systému včas plniť svoje poslanie za prítomnosti útokov, zlyhaní alebo nehôd (Linger, 2002)
- Kľúčové vlastnosti životaschopného OS:
  - odolnosť voči útokom
  - rozpoznávanie útokov a následných škôd
  - obnova základných služieb po útoku
  - prispôsobenie a vývoj ochranných mechanizmov systému na zmiernenie budúcich útokov

Úrovne ochrany

- v prípade narušenia systému nemožno dôverovať integrite súborov v systéme a ich údajom
- správca systému vyhodnocuje riziko narušenia podľa typu systému a jeho použitia:
  - izolovaný počítač bez internetu
    - vysoký stupeň ochrany s nízkym rizikom
    - Možné prieniky: prezradenie hesla, vírus
  - počítač v lokálnej sieti bez internetu
    - stredný stupeň ochrany so stredným rizikom
    - Možné prieniky: Snifers, Spoofing, prezradenie hesla, virus
  - lokálna sieť s internetom
    - nízky stupeň ochrany s vysokým rizikom
    - Možné prieniky: E-mail, webové služby, Snifers, Spoofing, prezradenie hesla, virus

Zálohovanie a obnova

- štandardný postup pre väčšinu systémov
- navrhnutie politiky a techniky pre zálohovanie
- možné automatické plánované zálohovanie
  - týždenné zálohovanie celého systému
  - denné zálohovanie údajov zmenených v ten deň
- uchovávanie záloh pre zvýšenie spoľahlivosti
  - 3 – 6 mesiacov mimo systému

- pri skorom zistení preniknutia administrátor obnoví poškodené údaje

Porušenie bezpečnosti

- medzery v systémovej bezpečnosti môžu aj nemusia byť škodlivé
  - niektoré prieniky sú výsledkom nevzdelaného používateľa a neoprávneného prístupu k systému
  - iné vniknutia ovplyvnia prevádzku systému
    - náhodné poruchy hardvéru, nezistené chyby v OS, prírodné katastrofy
- vážne poškodzujú dôveryhodnosť systému
- poznáme niekoľko známych porušení bezpečnosti

Úmyselné útoky

- patria sem:
  - útoky odmietnutia služby, prehliadanie, odpočúvanie, opakované pokusy, zadné vrátka, zber koša
- iný typ útoku do organizácie ako napr. vírus
- príkladom môže byť zle zobraté vyhodenie zamestnanca

Úmyselný neoprávnený prístup

- **Opakované pokusy**
  - vstup do systému formou uhádnutia hesla // *NBU123*
  - prelomenie formou výpočtu Brute-force alebo schémou fráz

Počet abecedných znakov	Počet možných kombinácií	Priemerný ľudský pokus (1s na pokus)	Priemerný čas pre počítač (1 milión/s)
1	26	13 s	0,000013 s
2	$26^2 = 676$	6 min	0,000338 s
3	$26^3 = 17\,576$	2,5 hod	0,008788 s
8	$26^8 = 208827064576$	6640 rokov	58 hod
10	$26^{10} = (1{,}4 \times 10)^{14}$	4,5 mil. rokov	4-5 rokov

Vírusy

- malý program napísaný s cieľom zmeniť spôsob fungovania počítača a jeho spustenia bez súhlasu alebo vedomia používateľa

- musí spĺňať:
  - musí sa vykonávať sám – cesta na spustenie iného programu
  - musí byť samoreplikovateľný – kopírovanie v systéme

Bezpečnostné koncepty v operačných systémoch

https://www.trellix.com/advanced-research-center/

Typy vírusov

- **Červy**
  - program v pamäti ktorý sa kopíruje bez potreby infikovaného súboru
  - odčerpáva systémové prostriedky
- **Trojský kôň**
  - deštruktívny program, ktorý je vydávaný za nejaký užitočný softvér
- **Logické bomby**
  - deštruktívny program, ktorého spúšťacím mechanizmom je udalosť, klávesa ...

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

Ochrana systému

- pôvod hrozby:
  - zvonku
  - vnútri v organizácií
- Spôsoby ochrany:
  - inštalácia antivírusového softvéru a jeho pravidelná aktualizácia
  - používanie brány firewall a jeho údržba
  - zabezpečenie prístupu neoprávneným osobám
  - vykonávanie šifrovania v systéme

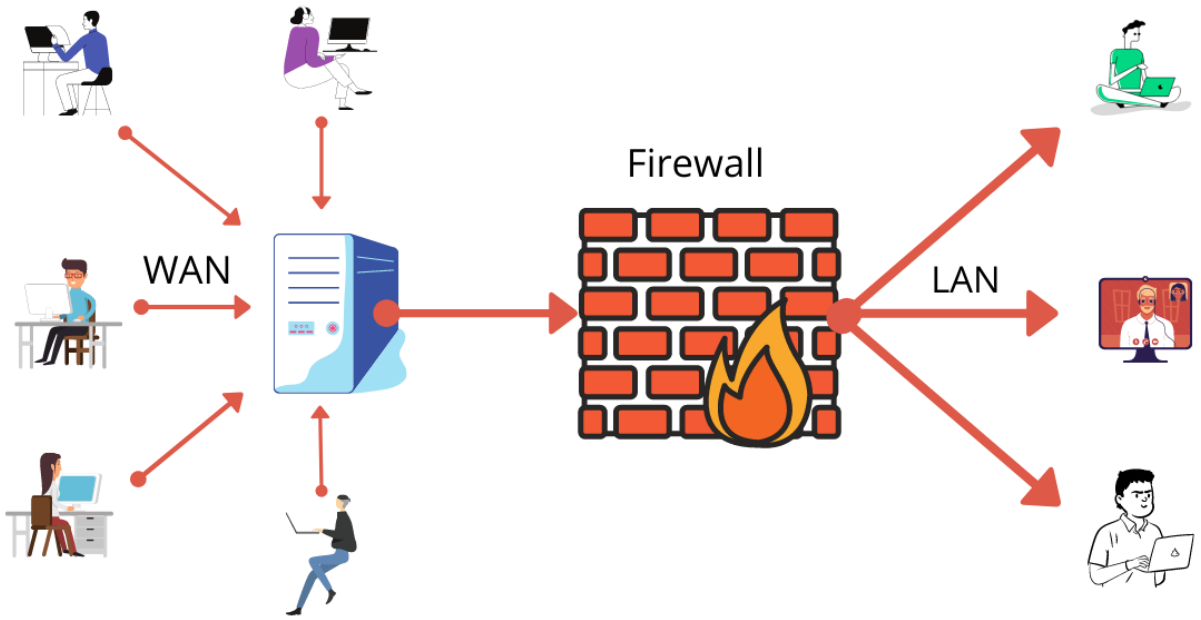
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Antivírus

- chráni systém pred škodlivým softvérom
- úroveň ochrany záleží od dôležitosti dát
  - medicínske dáta sú vysoko chránené
  - fotky a hudba by nemali byť v rovnakej úrovni zabezpečenia
- môže fungovať:
  - preventívne – vykonávanie kontrolného súčtu a porovnávanie
  - diagnosticky – kontroluje veľkosť súborov a pridaný kód

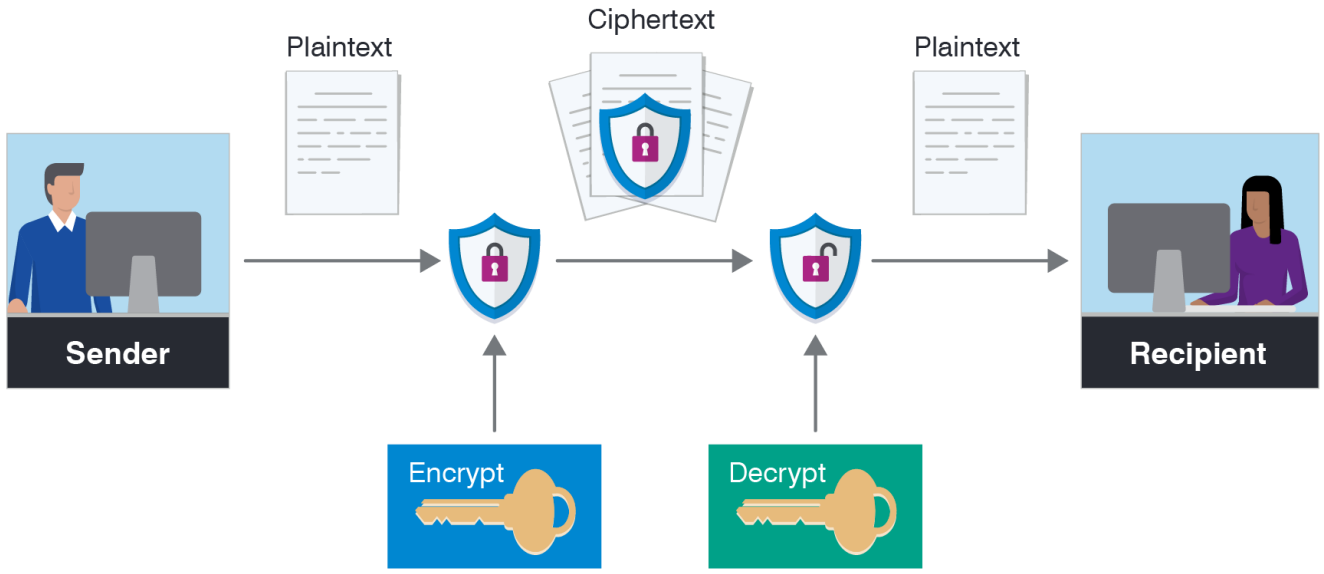
Firewall

- bráni proti sieťovým útokom
- hardvér alebo softvér navrhnutý na ochranu systému maskovaním IP adresy



Šifrovanie

- najextrémnejší spôsob ochrany údajov
- šifrovaná komunikácia v sieti – najbezpečnejší spôsob
- Nevýhodou je zvýšená réžia systému a spôsob výberu typu šifrovania



Different keys are used to encrypt and decrypt messages

Správa hesiel

- základný princíp ochrany hardvéru je dobre zvolené heslo
- mnoho používateľov zabúda heslo a preto ho neradi menia

- **Konštrukcia hesla:**
  - najefektívnejší a nejednoduchší systém ochrany systému
    - pri správnom použití
  - dobre zapamätateľné heslo sa musí často meniť
  - kombinácia znakov a čísel
  - nikdy neukladáme do skriptu pre pripojenie do siete

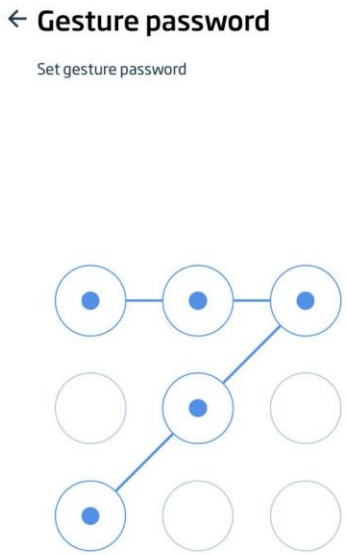
Technika generovania hesla

- existuje niekoľko techník na generovanie dobrého hesla:
  - používanie minimálne 8 znakov vrátane čísel a symbolov
  - vytvorenie nesprávne zapísaného slova alebo spojenie slova s frázou pre jednoduché zapamätanie
  - podľa určitého vzoru na klávesnici vygenerujete ľahko sekvenciu, zakaždým s iným písmenom
  - vytvorenie akronymov z citátov alebo viet
    - napr: MDWB4YOIA - My Dog Will Be 4 Years Old In April
  - rozlišovanie malých a veľkých písmen
    - napr: MDwb4YOia
  - nepoužívať slová zo slovníka

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

Alternatívy hesla

- alternatíva k heslám:
  - prístupové karty, kalkulačky hesiel
  - biometrické overovanie – odtlačok prsta, tvár, rozmer ruky, sietnica, hlas
  - heslo zadávané gestom na dotykovej obrazovke



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

Sociálne inžinierstvo

- získanie prístupu na základe:
  - predvolené heslo
  - zadné dvierka na hesle
  - heslo nájdene pri pokusoch v slovníku
  - sociálne inžinierstvo
- sledovanie prostredia – používateľského stola a hľadanie čo by mohlo používateľovi pripomínať prihlasovacie údaje
  - možné využitie aj kontaktovanie priateľov cez telefón zistenie
    - mená rodinných príslušníkov, domácich miláčikov, dovolenkových destinácií, koníčkov, modelov aut....
- **Phishing**
  - jednou z foriem, kde sa „votrelec“ vydáva za legitímnu entitu a kontaktuje neopatrných používateľov so žiadosťou o potvrdenie hesla, osobných informácií alebo finančných

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

Ochrana proti škodlivému kódu a nežiaducemu obsahu

Technické opatrenia (Blok IV)

Kurz: Manažér kybernetickej bezpečnosti

doc. Ing. Gabriel Koman, PhD.

doc. Ing. Jozef Kostolný, PhD.

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

gabriel.koman@uniza.sk

jozef.kostolny@uniza.sk