Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

# Základy identifikácie, autentizácie a autorizácie

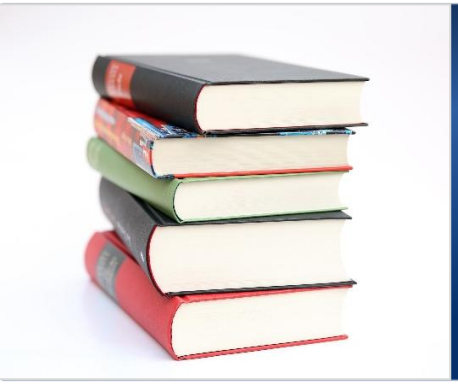
Identifikácia a autentizácia (Blok III)

**Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti**


doc. Ing. Gabriel Koman, PhD.

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

gabriel.koman@uniza.sk



- Základné pojmy a definície AAA
- Význam AAA vo verejnej správe
- Identifikácia používateľov a digitálna identita
  - prečo je dôležité chrániť svoju digitálnu identitu
  - ako sa využíva digitálna identita

# Základné pojmy a definície AAA

## Základné procesy na zabezpečenie správneho prístupu a ochrany údajov

# Identifikácia

- **Proces** zisťovania systémom, kto resp. aký subjekt sa pokúša o prístup k nejakému zdroju alebo službe
  - Subjekt požaduje prístup k systémovému prostriedku
- Subjekty majú pridelený jedinečný identifikátor (používateľské meno)
  - Identifikátor má identifikovať subjekt resp. používateľa
  - Používateľské meno je najbežnejšou metódou používanou na identifikáciu používateľa
  - Používateľské meno – kombinácia alfanumerických znakov, osobné identifikačné číslo, čipová karta, biometrické údaje
- Prvý krok v procese ochrany prístupu k citlivým údajom

- **Príklad**: Pri prihlásení do e-mailovej služby je zadaná e-mailovú adresa. Tento krok je identifikácia.



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

# Authentication (Autentifikácia)

- **Proces** overenia, či osoba alebo zariadenie, ktoré sa identifikovalo je skutočne tým, za ktoré sa vydáva
- Heslá sú najpoužívanejšou metódou na autentifikáciu
  - Prístupová fráza, prístupový kód, prístupový kľúč alebo PIN sa všeobecne označujú ako heslo
  - Heslo je reťazec znakov používaný na preukázanie identity používateľa

  - **Príklad:** Po zadaní e-mailovej adresy do systému je potrebné zadať aj heslo. Tento krok je autentizácia.

# Authentication (Autentifikácia)

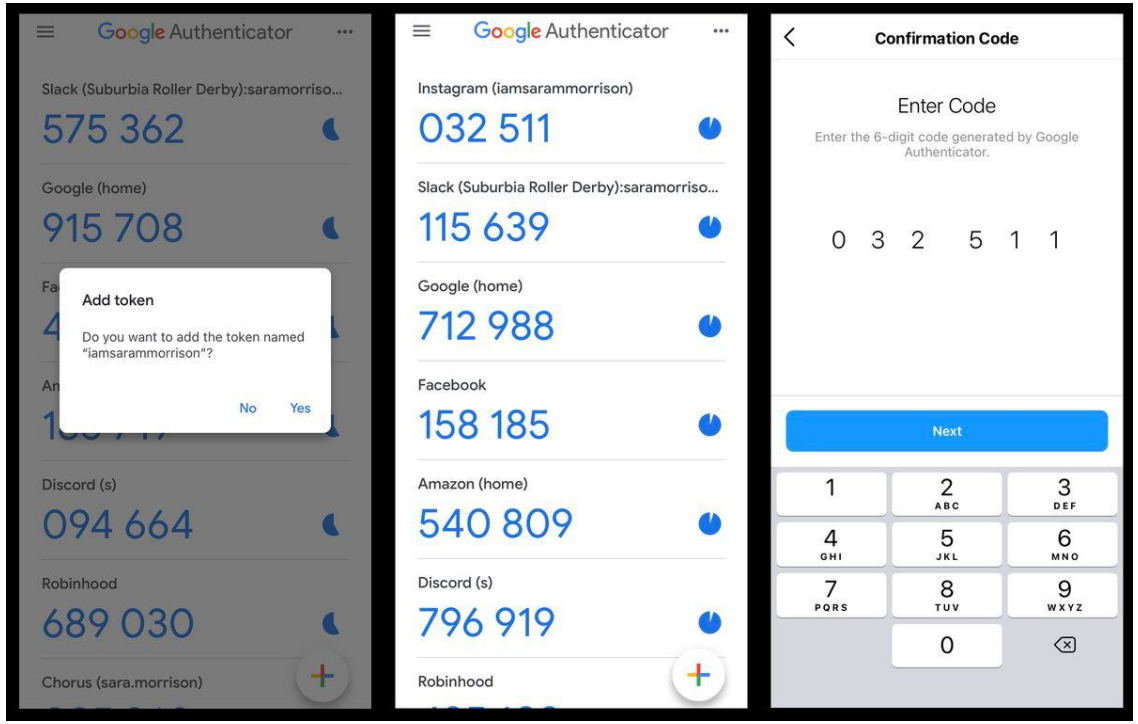
- Biometrické zabezpečenie:
  - Jedinečná fyzická charakteristika, ako je odtlačok prsta, sietnica alebo hlas, ktorá identifikuje konkrétneho používateľa
  - Porovnáva fyzické charakteristiky s uloženými profilmi na autentifikáciu používateľov
    - Profil je dátový súbor obsahujúci známe charakteristiky jednotlivca
    - Systém udelí používateľovi prístup, ak sa jeho charakteristiky zhodujú s uloženými nastaveniami
    - Čítačka odtlačkov prstov je bežné biometrické zariadenie
  - Biometria sa stáva čoraz populárnejšou v systémoch verejnej bezpečnosti, spotrebnej elektronike a aplikáciách na mieste predaja



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

# Authentication (Autentifikácia)

- **Viacfaktorová autentifikácia (2FA)** – bezpečnostný proces, pri ktorom musia používatelia poskytnúť dva rôzne autentifikačné faktory na overenie svojej identity a prístup k svojmu účtu(napr. bezpečnostný kľúč – kombinácia čo vieš, čo máš a kto si)
  - Lepšia ochrana osobných informácií používateľa jeho poverení a ďalších aktív
  - Zlepšuje aj bezpečnosť okolo zdrojov, ku ktorým má používateľ prístup
- Okrem používateľského mena a hesla alebo osobného identifikačného čísla (PIN) vyžaduje 2FA druhý token na overenie identity používateľa.
  - Týmto tokenom môže byť:
    - Fyzický objekt, ako je kreditná karta, mobilný telefón alebo kľúč
    - Biometrické skenovanie, ako je odtlačok prsta alebo rozpoznávanie tváre a hlasu
    - Overovací kód zaslaný prostredníctvom SMS, e-mailu alebo OTP aplikácie.



# Authentication (Autentifikácia)

- **Viacfaktorová autentifikácia (2FA)**
  - Dodatočná metóda zabezpečenia
  - Poskytuje vyššiu úroveň zabezpečenia ako autentifikačné metódy, ktoré sa spoliehajú iba na jeden autentifikačný faktor (jednofaktorová autentifikácia)
  - Jednofaktorová autentifikácia:
    - Používateľ poskytuje iba jeden faktor (zvyčajne heslo alebo PIN)
  - **Význam:**
    - Ak útočník pozná heslo používateľa, nebude mať prístup k jeho online účtu alebo mobilnému zariadeniu
  - V skutočnosti sa dvojfaktorová autentifikácia už dlho používa na kontrolu prístupu k citlivým údajom a systémom
  - **Odporúčanie:**
    - Aktivovať dvojfaktorovú autentifikáciu na všetkých vašich online účtoch, počítačoch a mobilných zariadeniach



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

# Authorization (Autorizácia)

- **Proces,** ktorý určuje konkrétne práva alebo úrovne prístupu používateľa po tom, ako sa úspešne identifikoval a autentifikoval
- Čo môže používateľ robiť, aké dáta si môže zobraziť, upraviť, aké akcie môže vykonať, ku ktorým sieťovým zdrojom má používateľ prístup a čo môže používateľ so zdrojmi robiť
- Autorizácia používa množinu atribútov, ktoré popisujú prístup užívateľa do siete
  - Systém porovnáva tieto atribúty s informáciami obsiahnutými v autentifikačnej databáze
  - Autorizácia je automatická a nevyžaduje, aby používatelia po overení vykonali ďalšie kroky
    - Implementujte autorizáciu ihneď po autentifikácii užívateľa

- **Príklad:** Po prihlásení do svojho účtu na sociálnej sieti môže používateľ upravovať svoj profil, pridať príspevky, ale nemá prístup k účtom ostatných používateľov.
  Tento krok je autorizácia.



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

# Accounting (Účtovanie)

- **Proces** zaznamenávania všetkých akcií a operácií, ktoré v systéme používateľ vykonáva
- **Využitie:**
  - Auditovanie
  - Monitorovanie prístupu k systémom
    - Detekcia bezpečnostných hrozieb
    - Detekcia podozrivej aktivity
  - Pomáha identifikovať neopravený prístup alebo zneužitie prístupových práv
  - Zabezpečenie integrity a dôveryhodnosti systémov
    - Každý krok v rámci systému je dokumentovaný a overiteľný
  - Zlepšenie reakcie na incidenty
    - Rýchle určenie pri zneužití systému, aké kroky boli vykonané a kedy sa udiali, čo pomáha pri analýze príčin a následkov incidentu.

- **Príklad:** Ak niekto upraví účet používateľa alebo získa prístup k jeho osobným údajom, tento zásah bude zaznamenaný v systéme. Tento záznam obsahuje informácie o tom, kedy a kto vykonal tieto zmeny, aké údaje boli upravené a z akého zariadenia lebo IP adresy sa prihlásil používateľ, ktorý zmenu vykonal. Tento krok je účtovanie.



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

# Význam v každodennom používaní internetu

- Základom bezpečnosti online účtov a dát
- Pri používaní rôznych služieb:
  - Online bankovníctvo
  - Sociálne siete
  - E-shopy...
- Zabezpečujú, že osobné údaje používateľa a finančné transakcie sú chránené pred neoprávneným prístupom
  1. **Identifikácia** – Zabezpečuje, že systém vie, kto sa prihlásil
  2. **Autentizácia** – Overuje, že sa to naozaj prihlásil konkrétny používateľ
  3. **Autorizácia** – Určuje, čo môže používateľ robiť
  4. **Účtovanie** – Sledovanie všetkých aktivít a operácií
- Bez týchto procesov by mohlo dôjsť k závažným bezpečnostným incidentom ako napr.:
  - Krádež identity
  - Finančné straty
  - Poškodenie reputácie



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

# Význam pri ochrane informačných systémov

- Kľúčové pre ochranu IS
  - Zabezpečujú, že len oprávnení používatelia môžu pristupovať k citlivým informáciám a vykonávať špecifické akcie v systémoch
  - Ochrana pred bezpečnostnými incidentmi ako napr.: úniky dát, kybernetické útoky alebo finančné straty
- Zabezpečenie prístupu
  - Autentifikácia - zabraňuje neoprávnenému prístupu k citlivým informáciám
  - Autorizácia - obmedzuje potenciálne škody
- Riadenie prístupových práv
  - Detailné riadenie prístupových práv - kľúčové pre ochranu citlivých dát a systémových zdrojov
- Sledovanie a auditovanie aktivít
  - Sledovanie potenciálnych bezpečnostných incidentov a analyzovanie ich príčiny
  - Neoceniteľné pri vyšetrovaní bezpečnostných incidentov
- Minimalizácia rizík
  - AAA znižujú riziko zneužitia privilégií, úniku dát a poškodenia systému



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

# Riziká bez AAA mechanizmov

- **Neoprávnený prístup a zneužitie údajov**
  - **Bez autentifikácie** môže ktokoľvek získať prístup k systému a dátam, čo vedie k vážnym bezpečnostným incidentom
    - Krádež identity, únik osobných alebo finančných údajov, manipulácia s dôležitými systémovými informáciami
- **Príklad:** Ak sa útočník bez vedomia používateľa prihlási do jeho online bankovníctva, môže zneužiť jeho údaje a vykonať neoprávnené platby alebo prevody peňazí.



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

# Riziká bez AAA mechanizmov

- **Zneužitie prístupových práv**
  - **Bez autorizácie** môžu používatelia s prístupom vykonávať akékoľvek akcie, vrátane tých, ktoré sú mimo ich právomocí, čo môže viesť k poškodeniu systému
  - Vážne dopady na integritu dát alebo môže spôsobiť právne a finančné problémy

- **Príklad:** Zlyhanie autorizácie môže umožniť zamestnancovi vykonať zmeny v systémových nastaveniach alebo prístup k citlivým údajom, ktoré nemá povolenie upravovať



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

# Riziká bez AAA mechanizmov

- **Nemožnosť sledovania aktivít**
  - **Bez účtovania** je nemožné zistiť, kto vykonal aké akcie v systéme, čo sťažuje vyšetrovanie bezpečnostných incidentov a umožňuje útočníkom skryť svoje stopy
  - Predlžuje reakčný čas na nápravu incidentu a môže zväčšiť rozsah škôd

- **Príklad:** Ak by neexistovali záznamy o prístupoch k databáze, nebolo by možné zistiť, kto a kedy zneužil systém a ukradol citlivé údaje



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

# Riziká bez AAA mechanizmov

- **Zvýšené riziko podvodov a bezpečnostných incidentov**
  - Ťažké odhaliť bezpečnostné incidenty:
    - Phishing
    - Krádeže prístupových údajov
    - Malware útok atď.
  - Útočníci môžu získať prístup k účtom a vykonávať škodlivé operácie bez toho, aby boli okamžite odhalení

- **Príklad:** Útoky typu "man-in-the-middle" alebo "phishing" môžu byť úspešné, ak nie sú implementované bezpečnostné opatrenia, ako sú silné metódy autentizácie, a zároveň neprítomnosť účtovania môže viesť k tomu, že podvod nebude včas odhalený.



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

# Príklady z reálneho života

- **Prihlásenie sa do e-mailu:**
  - Identifikácia
    - Zadanie používateľského mena alebo e-mailovú adresu
  - Autentifikácia
    - Zadanie hesla – jednofaktorová autentizácia
    - Prípadne ďalší kód ak sa používa 2FA
  - Autorizácia
    - Po úspešnom prihlásení systém určí, čo všetko je možné s e-mailovým účtom robiť
      - Čítať správy, meniť nastavenia účtu atď.
  - Účtovanie
    - Zaznamenávanie prístupov, času, lokality, zariadenia



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

# Príklady z reálneho života

- **Prihlásenie do internetového bankovníctva:**
  - Identifikácia
    - Zadanie používateľského mena alebo e-mailovej adresy
  - Autentifikácia
    - Zdanie hesla
    - Často je pridaný aj druhý krok autentifikácie, napríklad kód zaslaný na mobilný telefón
  - Autorizácia
    - Po úspešnej autentifikácii systém určí, aké akcie môže používateľ vykonávať
      - Zobraziť zostatok, vykonať prevod peňazí, systém si môže vyžiadať ďalšie potvrdenie, napríklad PIN alebo bezpečnostný kód
  - Účtovanie
    - Všetky tvoje transakcie, ako aj prístupy k účtu, sú zaznamenané
      - Ak by došlo k neautorizovanej transakcii, tieto záznamy pomôžu banke zistiť, kto vykonal daný prevod, kedy a z akého zariadenia



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

# Príklady z reálneho života

- **Použitie bankomatu:**
  - Identifikácia
    - Vloženie bankomatovej karty
  - Autentifikácia
    - Zadanie PIN kódu
  - Autorizácia
    - Po overení PIN kódu bankomat overí, či má používateľ dostatok finančných prostriedkov na výber hotovosti alebo na vykonanie inej transakcie
  - Účtovanie
    - Bankomat zaznamenáva všetky transakcie
      - Čas, miesto a suma výberu
        - Sledovanie finančných transakcií a na prevenciu podvodov

# Príklady z reálneho života

- **Prihlásenie do sociálnych sietí (napr. Facebook, Instagram):**
  - Identifikácia
    - Zadanie e-mailu alebo telefónneho čísla
  - Autentifikácia
    - Zadanie hesla
    - Možné využitie 2FA - systém pošle kód na mobilný telefón alebo do aplikácie, ktorý je potrebné zadať na potvrdenie prihlásenia
  - Autorizácia
    - Po prihlásení určí systém, aké akcie je možné vykonávať
      - Pridať príspevky, komentáre, zmena nastavenia účtu atď.
  - Účtovanie
    - Prístupy, ako aj interakcie (príspevky, komentáre) používateľa sú zaznamenávané, aby bolo možné identifikovať podozrivé aktivity
      - Napr.: prihlásenie z neznámeho zariadenia



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

# Príklady z reálneho života

- **Vstup do budovy s kartou:**
  - Identifikácia a autentifikácia
    - Priloženie prístupovej karty k čítačke
  - Autorizácia
    - Systém overí, či má karta oprávnenie na vstup do danej budovy alebo priestoru
  - Účtovanie
    - Systém zaznamenáva každý vstup, vrátane času a identifikácie osoby

# Význam AAA vo verejnej správe

**Zabezpečenie dôvery občanov a dodržiavanie zákonov o ochrane osobných údajov.**

# Význam AAA pre ochranu citlivých údajov a systémov vo verejnej správe

- Verejná správa spravuje a uchováva **množstvo citlivých údajov**:
  - Osobné informácie občanov
  - Štátne tajomstvá
  - Daňové údaje
  - Zdravotné záznamy
  - Právne dokumenty a pod.
- **Implementácia AAA mechanizmov:**
  - Kľúčové pre ochranu informácií pred rôznymi bezpečnostnými hrozbami
  - Zabezpečenie údajov pred neoprávneným prístupom, zneužitím alebo stratou
  - Zabezpečenie dôvery občanov
  - Dodržiavanie zákonov o ochrane osobných údajov



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

# Význam AAA pre ochranu citlivých údajov a systémov vo verejnej správe

- **Ochrana citlivých údajov**
  - Osobné údaje občanov, zdravotné záznamy, daňové informácie, právne dokumenty alebo údaje týkajúce sa verejných financií
  - **Identifikácia**
    - Každý používateľ alebo zamestnanec verejnej správy je riadne identifikovaný pred tým, ako získa prístup k citlivým informáciám
      - Systém vie, kto sa pokúša o prístup a môže okamžite identifikovať potenciálnych útočníkov alebo neoprávnené osoby
  - **Autentifikácia**
    - Overenie používateľa a potvrdenie, že je to skutočne tá osoba, ktorá sa hlási do systému
      - Zabraňuje, aby neautorizovaní používatelia získali prístup k dôležitým a citlivým údajom
  - **Autorizácia**
    - Používateľ bude mať prístup iba k tým údajom a systémom, ktoré sú mu povolené
      - Predchádzanie zneužitia prístupových práv, a zároveň nie každý zamestnanec môže pristupovať ku všetkým údajom
  - **Účtovanie**
    - Všetky operácie vykonané v systéme
      - Spätná analýza v prípade podozrivých aktivít, ako je neoprávnený prístup alebo manipulácia s údajmi



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

# Význam AAA pre ochranu citlivých údajov a systémov vo verejnej správe

- **Zabezpečenie práv občanov a ochrana pred zneužitím práv**
  - Verejná správa je zodpovedná za spravovanie údajov občanov a iných subjektov, pričom tieto údaje majú právny význam
  - **Identifikácia a autentifikácia**
    - Údaje o občanoch a ich práva sú chránené a iba oprávnení úradníci môžu manipulovať s citlivými informáciami
      - Daňové priznania, rodné listy, občianske preukazy alebo iné verejné dokumenty
  - **Autorizácia**
    - Každý zamestnanec v rámci verejnej správy má prístup iba k tým informáciám, ktoré sú nevyhnutné na výkon jeho práce
    - Zvyšovanie transparentnosti a zodpovednosti verejnej správy sledovaním aktivity používateľov
      - Príklad: Pracovník na daňovom úrade môže mať prístup k daňovým údajom, ale nie k zdravotným záznamom občanov
  - **Účtovanie**
    - Zaručuje, že všetky operácie týkajúce sa zmeny alebo prístupu k osobným údajom sú zaznamenávané a môžu byť skontrolované

# Význam AAA pre ochranu citlivých údajov a systémov vo verejnej správe

- **Zabezpečenie dôvery občanov vo verejné inštitúcie**
  - AAA preukazujú, že štátne inštitúcie vynakladajú úsilie na ochranu osobných údajov a zamedzujú neoprávnenému prístupu
  - **Identifikácia a autentifikácia**
    - Istota, že systém správne overí identitu občana a že jeho osobné údaje budú chránené pred neoprávneným prístupom
  - **Autorizácia**
    - Zamestnanci verejných inštitúcií majú prístup len k informáciám, ktoré sú nevyhnutné pre ich prácu
      - Minimalizuje sa riziko zneužitia údajov
  - **Účtovanie**
    - Umožňuje občanom a regulačným orgánom skontrolovať, kto mal prístup k ich údajom a čo s nimi vykonával
      - Zvyšuje sa transparentnosť a dôvera v systémy verejnej správy



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

# Význam AAA pre ochranu citlivých údajov a systémov vo verejnej správe

- **Zníženie rizika kybernetických útokov a zneužitia útočníkmi**
  - AAA pomáha minimalizovať riziko kybernetických útokov tým, že poskytuje ochranu prístupu a monitorovanie aktivít v systémoch
  - **Identifikácia a autentifikácia**
    - Zabránenie neoprávneným osobám v prístupe k databázam a systémom verejnej správy
  - **Autorizácia**
    - Ak sa útočníkovi podarí získať prístup do systému, nemôže vykonávať operácie, ktoré sú mimo jeho oprávnení
  - **Účtovanie**
    - V prípade kybernetického útoku:
      - Rýchle identifikovanie zraniteľnosti v systéme
      - Odsledovanie, ako útok prebiehal, čo pomáha pri jeho eliminovaní a prevencii v budúcnosti



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

# Význam AAA pre ochranu citlivých údajov a systémov vo verejnej správe

- **Nevyhnutné pre ochranu citlivých údajov a systémov vo verejnej správe**
- Zabezpečujú, že:
  - Osobné a citlivé údaje občanov sú chránené pred neoprávneným prístupom
  - Zneužitie prístupových práv je minimalizované, čo zaručuje správne spravovanie práv občanov
  - Dôvera verejnosti v štátne inštitúcie je posilnená prostredníctvom transparentnosti a ochrany súkromia
  - Riziko kybernetických útokov je znížené a môže byť efektívne monitorované a analyzované



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

# Príklady použitia AAA pre ochranu údajov a systémov vo verejnej správe

- **Slovensko.sk**
  - elektronický občiansky preukaz
    - BOK - kód chrániaci prístup k elektronickému obsahu preukazu (certifikáty)
    - KEP - kvalifikovaný elektronický podpis (ekvivalent podpisu rukou)
    - KEP PIN - kód chrániaci prístup ku KEP

- **Sociálna poisťovňa**
  - prihlásenie
    - elektronický občiansky preukaz
    - Meno a heslo + druhý faktor OTP kód

- **Štátna pokladnica**
  - prihlásenie
    - Meno a heslo + druhý faktor bezpečnostný token

# Identifikácia používateľov a digitálna identita - prečo chrániť digitálnu identitu a ako sa využíva

# Digitálna identita

- Digitálna identita je **súhrn všetkých informácií** a dát, ktoré identifikujú osobu **v online prostredí**

- Predstavuje **elektronický ekvivalent osobnosti** a obsahuje informácie o aktivitách, preferenciách a údajoch, ktoré o osobe existujú na internete

- Digitálnu identitu tvoria:
  - Osobné údaje (meno, priezvisko, dátum narodenia, e-mail, telefónne číslo)
  - Online aktivity (vyhľadávania, navštívené webové stránky, zdieľaný obsah, nákupy, ...)
  - Technické údaje (IP adresa, typ zariadenia, prehliadač, ...)
  - Digitálne certifikáty (verejný a súkromný kľúč)

# Ako chrániť digitálnu identitu

- **Používajte silné a unikátne heslá** – Každý účet by mal mať svoje vlastné zložité heslo, ktoré je ťažké uhádnuť. Ideálna je kombinácia písmen, čísel a špeciálnych znakov. Heslo si nikdy nezapisujte, ale ukladajte pomocou správcu hesiel.
- **Zapínajte dvojfaktorové overenie (2FA)** – Nastavenie dvojfaktorového overenia pridáva ďalšiu vrstvu zabezpečenia, takže aj keď niekto získa vaše heslo, bez druhého kroku (napríklad kódu v SMS alebo v aplikácii) sa k dátam nedostane.
- **Pravidelne aktualizujte softvér a aplikácie** – Pravidelné aktualizácie operačných systémov a aplikácií opravujú bezpečnostné chyby, ktoré môžu hackeri využiť. Preto ich nikdy neodkladajte.
- **Buďte opatrní na phishing** – Nikdy neklikajte na odkazy alebo neotvárajte prílohy v podozrivých e-mailoch. Skontrolujte vždy odosielateľa a radšej navštívte oficiálne webové stránky ručne, než kliknutím na odkaz v e-maile, ktorý sa vám nezdá.



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

# Ako sa využíva digitálna identita

- **Autentifikácia a autorizácia**: Digitálna identita umožňuje overiť, či ste naozaj tým, za koho sa vydávate, a či máte oprávnenie pristupovať k určitým informáciám alebo službám.

- **Online služby**: Môžete ju použiť na prihlásenie do e-mailu, sociálnych sietí, online bankovníctva, alebo na prístup k vládnym portálom a službám.

- **Offline služby**: Digitálnu identitu je možné použiť aj v offline prostredí, napríklad na preukazovanie totožnosti pri interakcii s verejnými inštitúciami alebo pri preberaní balíkov.



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

# Ako sa využíva digitálna identita

- **Ukladanie a zdieľanie digitálnych dokumentov:** Umožňuje bezpečné ukladanie a zdieľanie digitálnych dokumentov, ako sú občianske preukazy, vodičské preukazy, diplomy, atď.

- **Digitálne podpisy:** Umožňuje vytvárať záväzné digitálne podpisy na zmluvách, žiadostiach a iných dokumentoch, čím nahrádza klasický podpis na papieri.

- Digitálna identita je teda komplexný koncept, ktorý v digitálnom svete nahrádza tradičné formy identifikácie a autorizácie, čím uľahčuje prístup k službám a zefektívňuje procesy.



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

# Otvorená reflexia

Aký je primárny cieľ identifikácie v rámci AAA?

A) Overenie hesla

B) Overenie identity osoby

C) Zistenie, kto žiada prístup

D) Prideľovanie prístupových práv

# Otvorená reflexia

Ktorý z nasledujúcich prvkov je príkladom identifikátora?

A) Heslo

B) PIN

C) Používateľské meno

D) E-mailová správa

# Otvorená reflexia

Aký typ autentifikácie predstavuje kombináciu hesla a biometrického odtlačku prsta?

A) Jednofaktorová

B) Trojfaktorová

C) Viacfaktorová

D) Zmiešaná autentifikácia

# Otvorená reflexia

Ktorý krok AAA procesu nasleduje po autentifikácii?

A) Účtovanie

B) Identifikácia

C) Autentifikácia

D) Autorizácia

# Otvorená reflexia

Vyberte pravdivé tvrdenie o autorizácii.

A) Určuje, či je používateľ prihlásený

B) Overuje identitu používateľa

C) Umožňuje používateľovi vykonávať akcie podľa pridelených práv

D) Zaznamenáva systémové udalosti

# Otvorená reflexia

Čo zaznamenáva accounting v rámci AAA?

A) Úroveň prístupu

B) Údaje o akciách vykonaných používateľom

C) Aktuálne heslo

D) Autentifikačné tokeny



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

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

## Základy identifikácie, autentizácie a autorizácie

Identifikácia a autentizácia (Blok III)

**Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti**

doc. Ing. Gabriel Koman, PhD.

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

gabriel.koman@uniza.sk