Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Autorizácia a riadenie prístupu

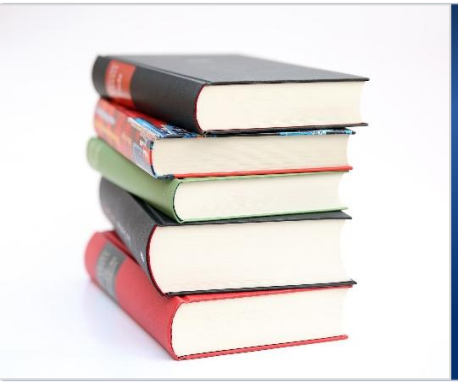
Autorizácia, monitorovanie a riešenie incidentov (Blok IV)

Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti

Pavel Segeč

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

Pavel.Segec@fri.uniza.sk



V dnešnej prednáške sa pozrieme na ...

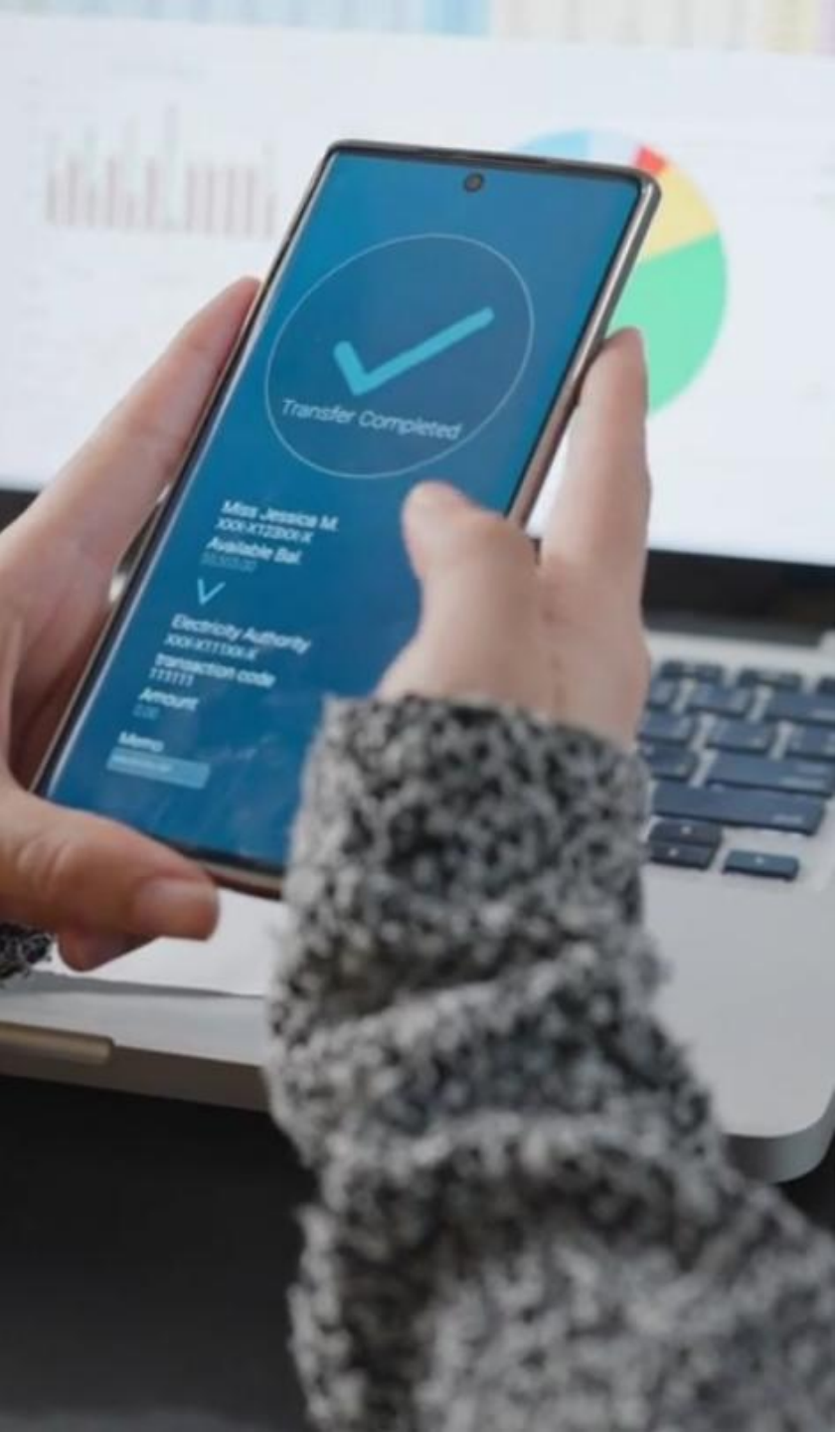
- Autentifikácia (Authentication) – krátke pripomenutie
- Autorizácia (Authorization)
- Modely autorizácie
- Systém riadenia prístupu (Access Control)
- Odporúčania – best practises

Dôvod dnešnej témy

Úvod - Prečo je téma autorizácie dôležitá?

- Súčasný trend = **digitalizácia**
  - Činnosti, kedysi robené ručne => presúvajú sa ***do digitálnej podoby***
    - Cez počítače, mobilné aplikácie alebo online služby.
    - **Príklad**: Namiesto fronty na úrade vybavím agendu cez internet (poistenie, preukazy, online parkovné, Slovensko.SK ...).
- **Potrebujeme riešiť bezpečnosť**
  - **Chrániť digitálne dáta pred zneužitím**
    - **Príklad:** Aby ktokoľvek nemohol meniť údaje na našom účte alebo čítať naše e-maily
  - **Zabezpečiť, že prístup majú len oprávnení ľudia**
    - Príklad:
      - **Lekár** môže vidieť a meniť diagnózu v zázname
      - **Administratívny** pracovník nie

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



Dôvod dnešnej témy

Úvod - Prečo je téma autorizácie dôležitá?

- **Potrebujeme riešiť bezpečnosť !!**
  - *Základným cieľom je*
    - ***zabrániť neoprávneným používateľom získať prístup k zdrojom***
    - ***zabrániť oprávneným používateľom pristúpiť k zdrojom neoprávneným spôsobom***
    - ***a umožniť oprávneným používateľom pristúpiť k zdrojom oprávneným spôsobom***

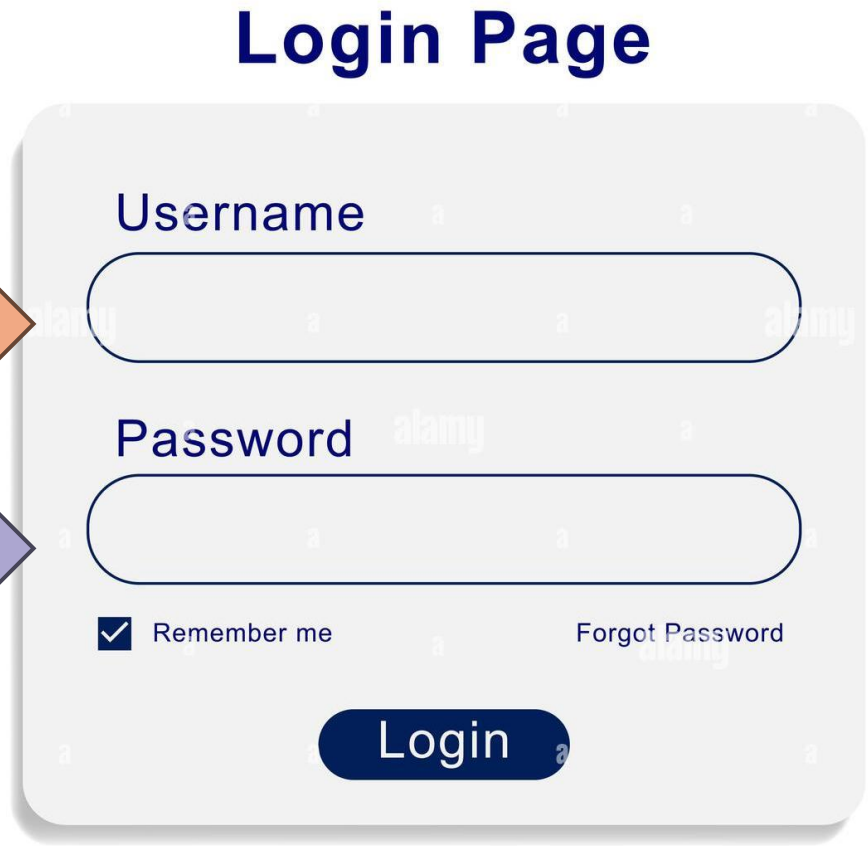
zdroj, doc. Hudec, FIIT STU

- ==> rieši **Autentifikácia** a **Autorizácia**
  - Kľúčové piliere kybernetickej bezpečnosti !!!!
  - Potrebujeme vedieť, kto je **kto** a čo **môže robiť**
    - Riadenie prístupu na základe identity používateľa alebo zariadenia

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

Identifikácia a autentizácia, autorizácia

- Pri prístupe k digitálnym zdrojom sa potrebujeme **Autentifikovať**
- **Autentifikácia pozostáva**
  - **Identifikácia (*identification*)**
    - Procedúra kde používateľ prezentuje svoju totožnosť
    - „Predstavujem“ sa systému kto som
      - Identifikujem sa ako jeho platný používateľ
      - Zadaním napr. e-mailovej adresy alebo mena
  - **Verifikácia (*verification*) alebo autentizácia**
    - Overenie, že som to naozaj ja
      - *Proces overenia totožnosti používateľa*
      - Zadaním napr. hesla alebo kódu zo SMS
      - Potvrdenie dôveryhodnosti Identity



Krátke pripomenutie - Autentizácia vs. Autorizácia

Identita a Digitálna identita

- **Identita** = **Kto sme**
  - Charakteristické znaky a vlastností osoby
  - Spôsob pre ostatných spoznať a overiť, že sme to my

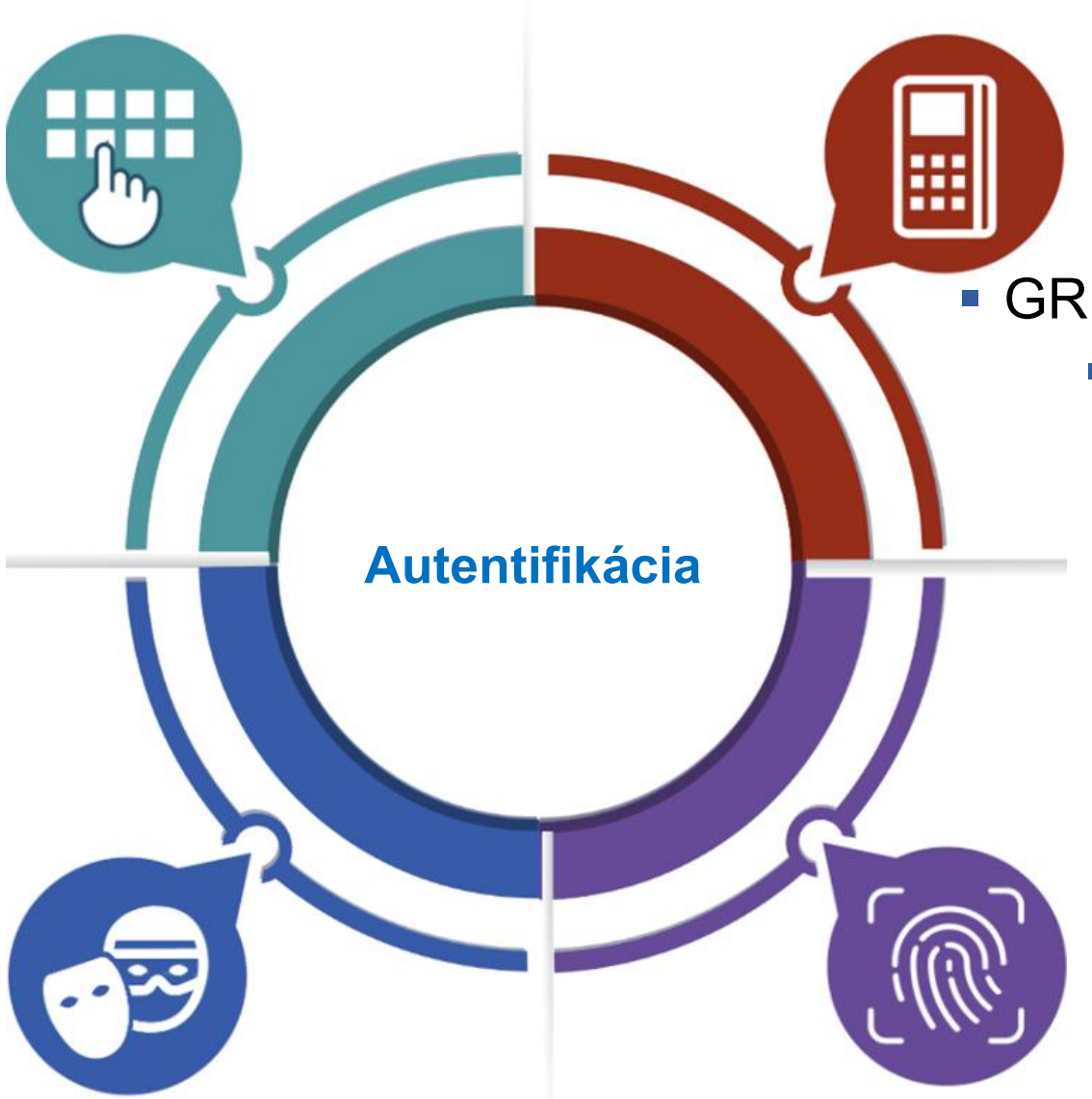
- Fyzický svet = **Fyzická identita** (bežná identita)
  - Totožnosť konkrétnej fyzickej osoby
  - **Príklady:** Občiansky preukaz, pas, vodičský preukaz, preukaz zamestnanca ...
  - **Overenie**: Pomocou dokumentov alebo údajov

- Online svet = **Digitálna identita**
  - Odlišovacia informácia (jedna alebo viac) o konkrétnom používateľovi
    - Online verzia našej identity v digitálnom svete
  - **Príklady:** Používateľské meno, e-mail adresa, telefónne číslo, unikátny identifikátor, rodné číslo, a iné.
  - **Overenie:** napr. zadaním mena a hesla pri prihlásení do online účtu

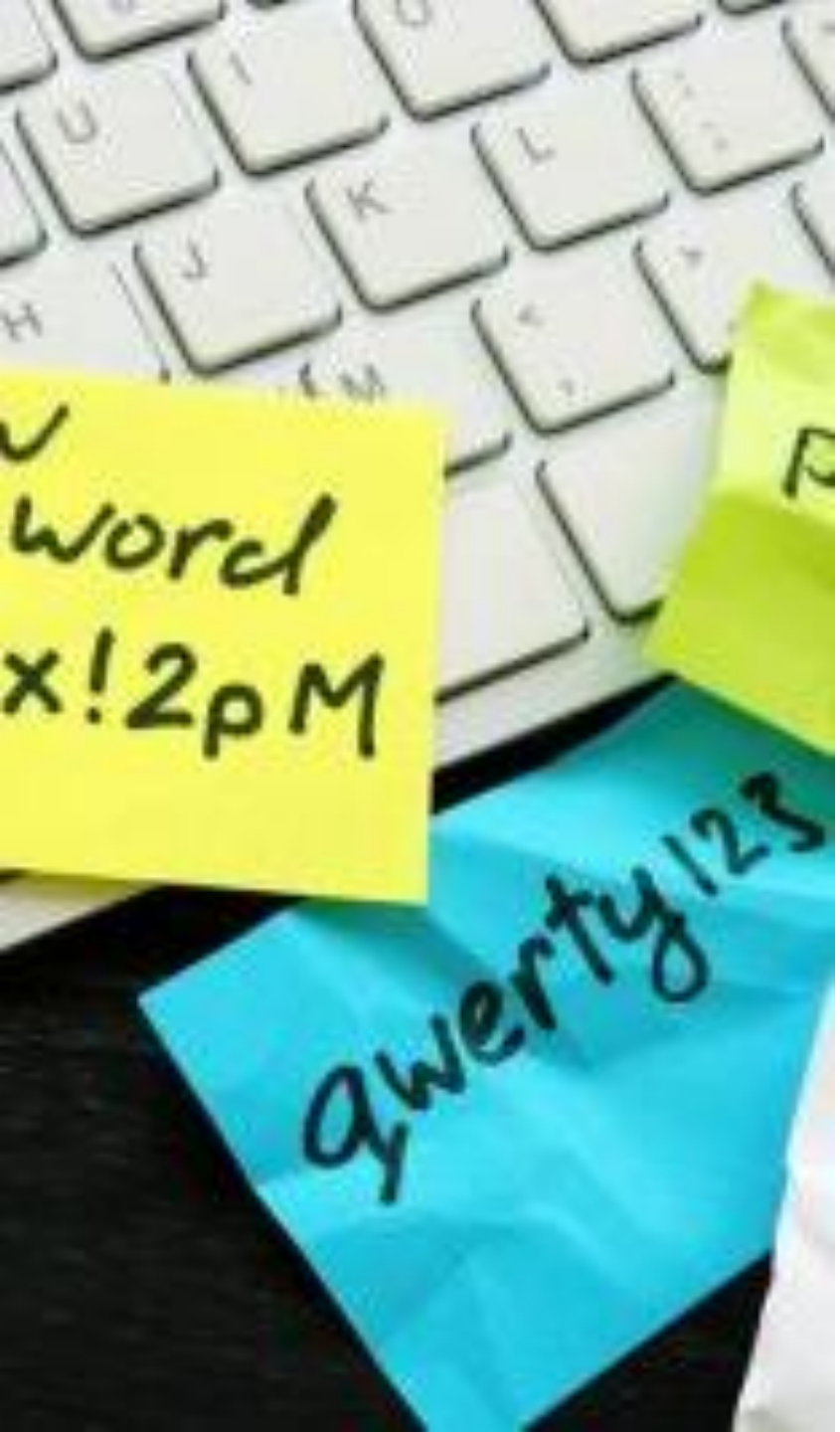
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Metódy autentifikácie

- **Niečo, čo viem len ja** (tajomstvo)
  - PIN
  - Heslo
  - Fráza
  - Kód
  - Jednorazové heslo
  - ...
- **Niečo, čo robím** (čo ma charakterizuje)
  - Ako rozprávam
  - Ako píšem na klávesnici
  - Pohyb myšou
  - Rukopis ...

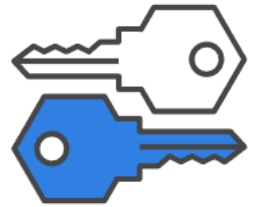


- **Niečo, čo mám / vlastním**
  - Mobil, SMS
  - GRID karta, platobná kartu
  - Čipová karta, ID karta
  - ...
- **Niečo, čo som** (moja jedinečná charakteristika)
  - Odtlačok prsta
  - Sken sietnice
  - Sken tváre
  - Veľkosť prsta/dlane
  - ....



Jedno a viacfaktorová autentifikácia

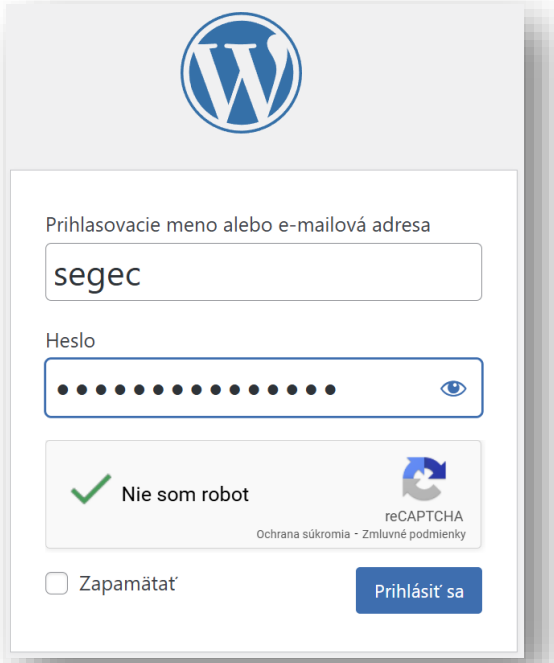
- **Jednofaktorová autentifikácia**
  - Používa jeden spôsob overenia totožnosti
  - V princípe, ak je **správne implementované a použitá**, môže poskytovať bezpečnú autentizáciu používateľa
  - Riziká:
    - Slabé heslá, opakované heslá, komplikovaný systém, pôsobenie útočníka ...
- Riešenie ==> **Dvoj (2FA) a viacfaktorová autentifikácia**
  - Navýšenie počtu faktorov
    - 🔑 Zadáš heslo (niečo, čo vieš)
    - 📱 Potvrdíš kód zo SMS alebo mobilnej aplikácie (niečo, čo máš)
  - Zníženie rizika krádeže identity
  - Bežné napr. v bankovníctve, štátnych portáloch, e-mailových službách



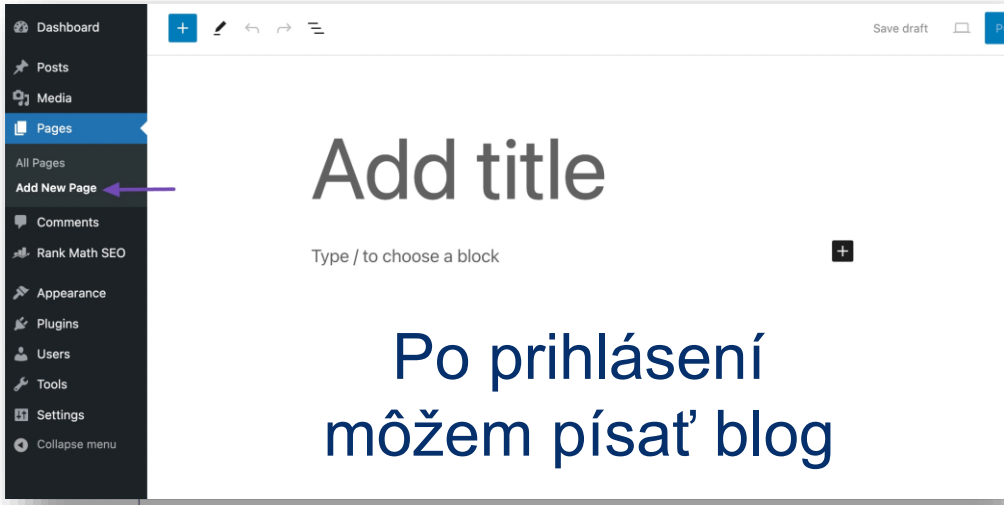
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Identifikácia, autentizácia, autorizácia

- Digitálne systémy pred začatím používania typicky od nás požadujú
  - Identifikáciu
    - Používateľ sa identifikuje do systému.
  - Autentizáciu (verifikáciu)
    - Systém overí používateľa na základe autentizačnej informácie



- **Autorizácia (čo môžem v systéme robiť)**
  - Určuje, k čomu máme prístup po úspešnom overení a prihlásení
    - ***Čo môžem robiť v systéme, ktorý ma autentizoval***
    - Práva určuje vlastník / organizácia
    - Nie používateľ



Po prihlásení môžem písať blog

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

Čo je teda autorizácia?

- **Autorizácia**
  - Proces, ktorý určuje, či má overený používateľ ***právo*** vykonať určitú akciu alebo pristupovať k určitému zdroju
    - Jednoducho:
      - Autorizácia rozhoduje, čo smieme robiť po prihlásení do systému
      - Určuje tzv. prístupové práva po overení identity

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

Prečo je autorizácia dôležitá?

- **Bezpečnosť** → Chráni citlivé údaje pred neoprávneným prístupom
- **Kontrola** → Zabezpečuje, že akcie vykonávajú len oprávnení používatelia
- **Súkromie** → Podporuje dodržiavanie bezpečnostných pravidiel

- Príklad čo autorizácia umožňuje:
  - Prihlásiť sa do mobilu / PC a používať ho
  - Prihlásiť sa do mobilu / PC a inštalovať programy
  - Povolenie čítať alebo upravovať dokumenty, dochádzku
  - Prihlásiť sa do aplikácie a používať ju
  - Písať alebo len čítať neverejné blogy, videá
  - V e-bankovom systéme autorizácia určuje, či môžete:
    - Zobraziť históriu platieb, Previesť peniaze, Upraviť nastavenia účtu

- *Autentizácia je ako ukázanie kľúča od dverí; autorizácia je, do ktorých miestností môžete vstúpiť*

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

Porovnanie: Autentizácia vs. Autorizácia

Kategória	Autentizácia	Autorizácia
Čo robí	Overuje identitu používateľa	Určuje úroveň prístupu používateľa
Čo to znamená	Dokazuje, že používateľ je ten, za koho sa vydáva	Overuje, k akým zdrojom má používateľ prístup
Kedy sa vykonáva	Ako prvý krok pred prístupom	Až po úspešnej autentizácii
Kto ju nastavuje	**Používateľ**	**Organizácia** (admin), vlastník zariadenia/systému
Ako funguje	Heslá, biometria, PINy, ...	Na základe nastavení vlastníka/organizácie
Príklad	Ukázanie občianskeho preukazu na vrátnici.	Povolenie vstupu do konkrétnych kancelárií.
	Prihlásenie do e-mailu	Povolenie posielať alebo mazať správy
Typy	Jednofaktorová, 2FA, MFA	ABAC, RBAC, MAC, DAC

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

Autorizácia - Otázka na zamyslenie

- **Otázka**:
  - Je zadanie hesla autentizácia alebo autorizácia?

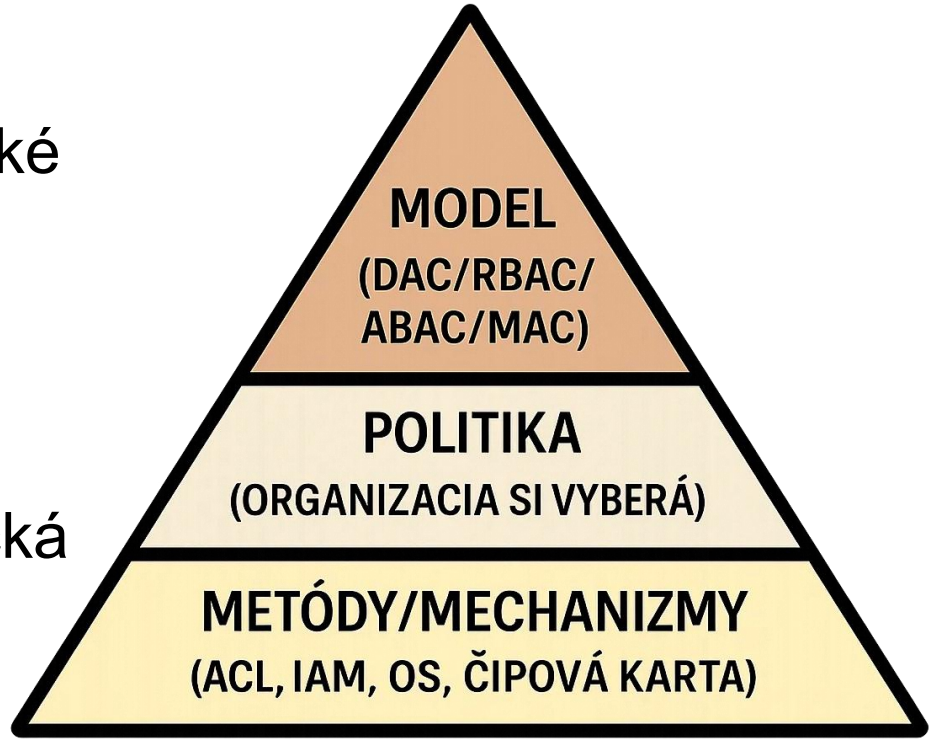
- **Otázka**:
  - Čo sa stane, ak máme autentizáciu, ale slabú autorizáciu?
    - V budove
    - Vo vašej aplikácií, na úrade ...

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

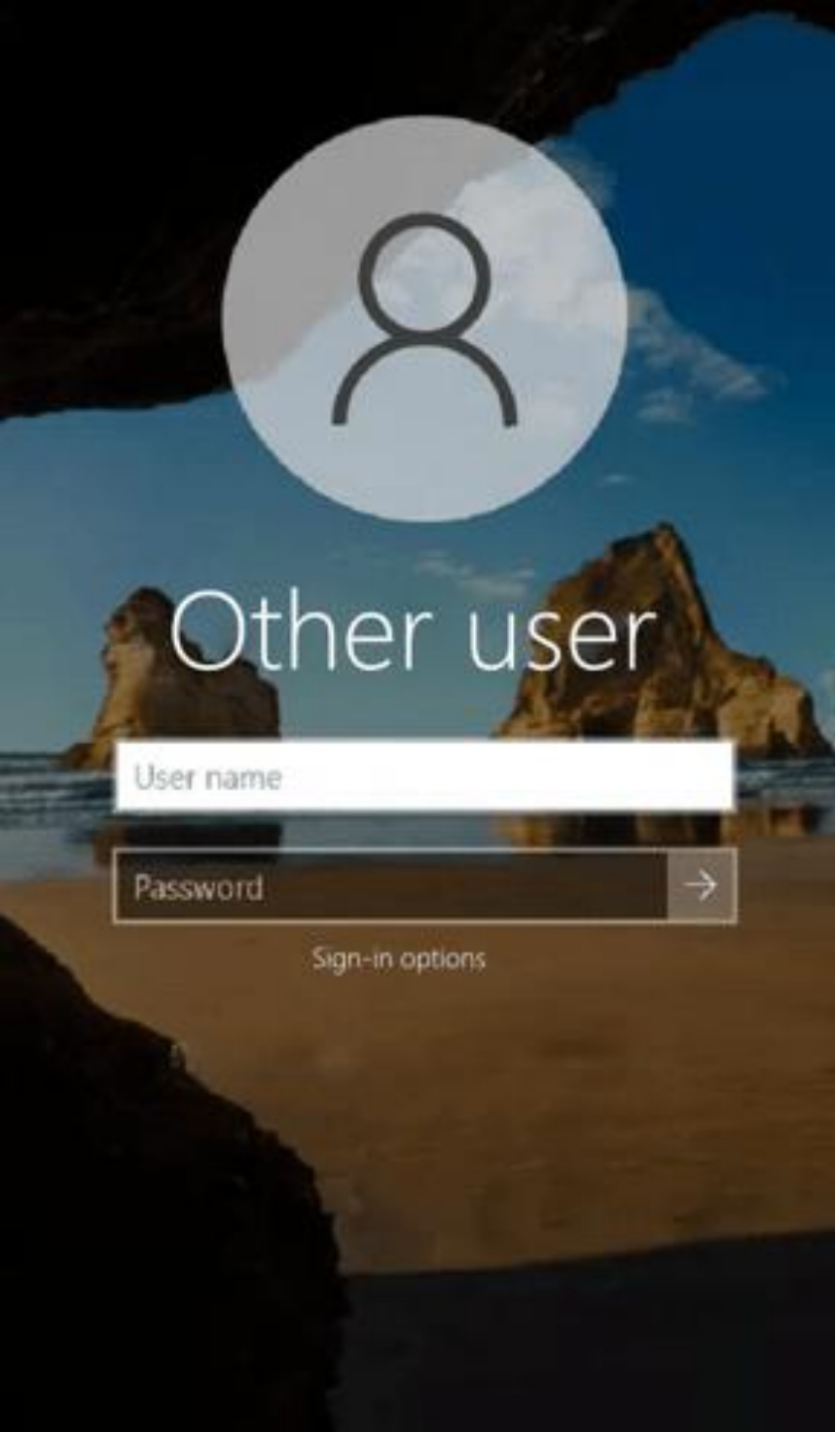
Autorizačné modely

Autorizačné modely, politiky a metódy

- **Ako sa implementuje autorizácia?**
  - **==>** Pomocou autorizačných modelov, metód a mechanizmov
  - **Autorizačný model** = **„filozofia / pravidlá**
    - Pravidlá podľa ktorých sa rozhoduje, kto má aké oprávnenia
    - *Pozn. dnes sa naň pozrieme*
  - **Politika** = **organizačné rozhodnutie**
    - Určuje aký model sa konkrétne použije
    - *Pozn. nebudeme sa tomu venovať*
  - **Autorizačná metóda / mechanizmus** = technická realizácia
    - Konkrétny nástroj, technika alebo postup
    - Akým systém rozhoduje o tom, aké práva máme
      - Čo smieme robiť po autentifikácii
    - *Pozn. nebudeme sa tomu venovať*



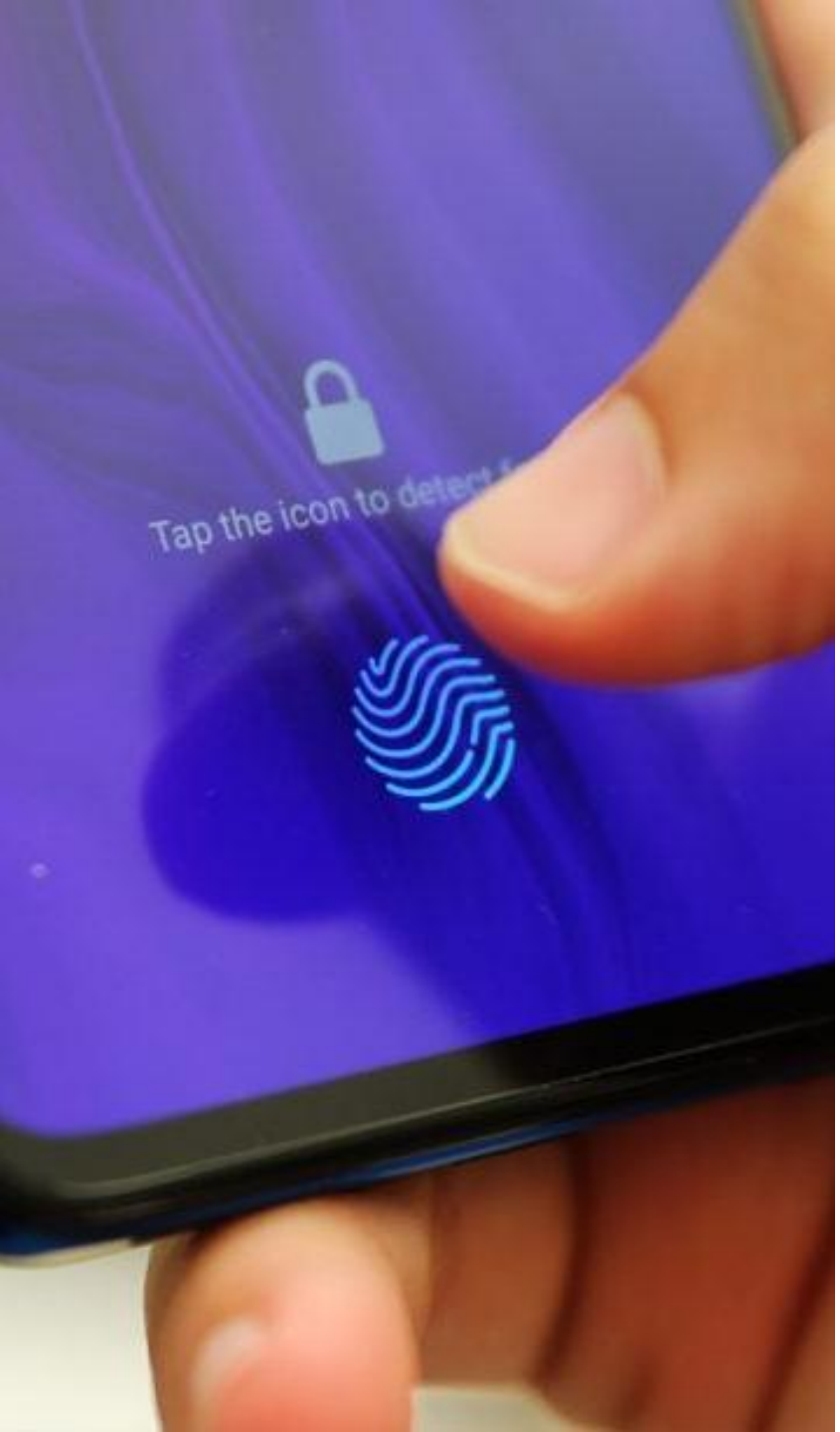
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE



Príklad autorizácie a jej model (1.)

- **Príklad:** Prihlásenie sa do firemného počítača
  - **Autentifikácia:**
    - Zadám svoje meno a heslo
    - Systém verifikuje kto som
  - **Autorizácia:**
    - Systém skontroluje moju rolu
      - **Bežný zamestnanec**
        - Môžem otvoriť e-maily a prezerať dokumenty
        - ale nemôžem inštalovať nové programy
      - **„IT administrátor“**
        - Môžem inštalovať programy a meniť nastavenia

Model: Práva sú priradené podľa role - autorizácia na základe rolí



Príklad autorizácie a jej model (2.)

- **Príklad:** Prihlasujem sa do mobilu
  - **Autentifikácia**
    - Použijem odtlačok prsta (sken tváre, vzor)
    - Systém potvrdí, že som to ja
  - **Autorizácia**
    - Systém rozhodne
      - **Som „hlavný používateľ“?**
        - Mám prístup ku všetkým aplikáciám a súborom
      - Je to **„hosťovský účet**“ pre niekoho iného?
        - Ten môže používať len základné funkcie
        - napr. volať, ale nemohol by otvoriť vaše fotky

Model : Práva sú priradené podľa role – autorizácia na základe rolí

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

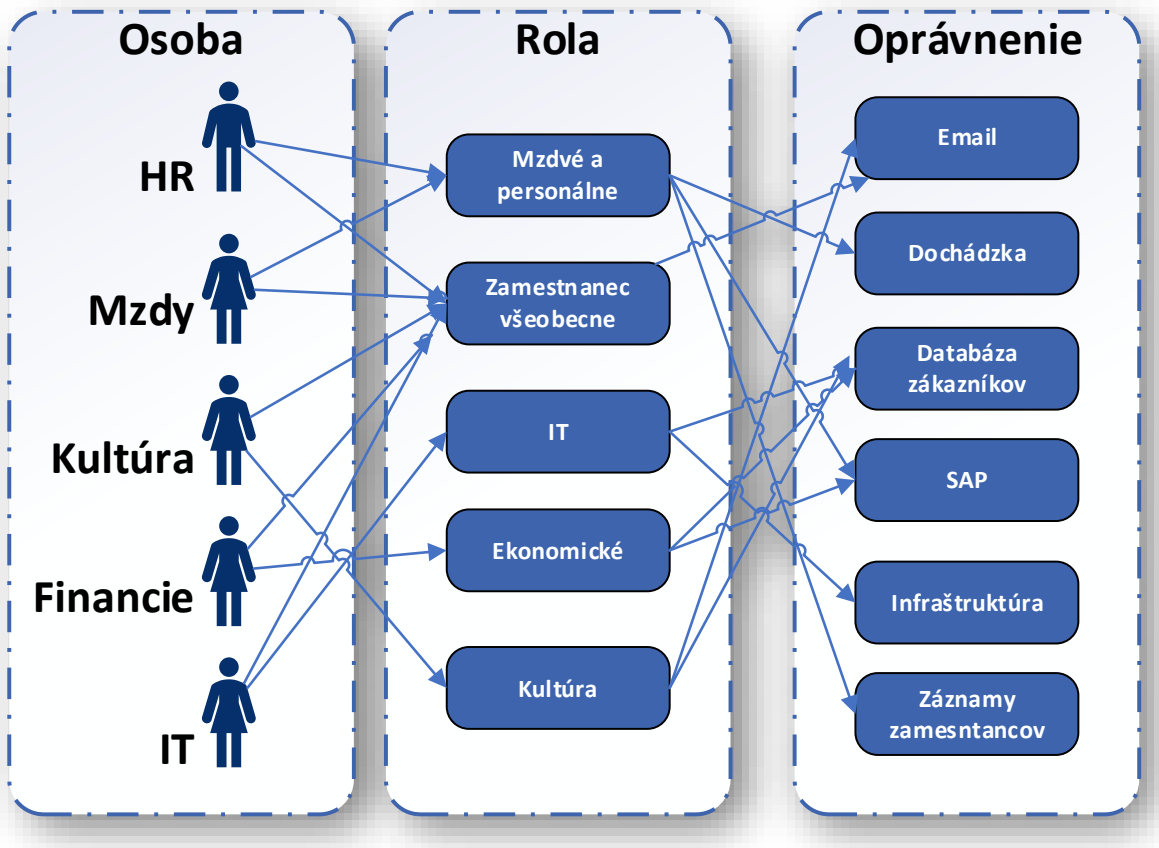
Otázka pre vás

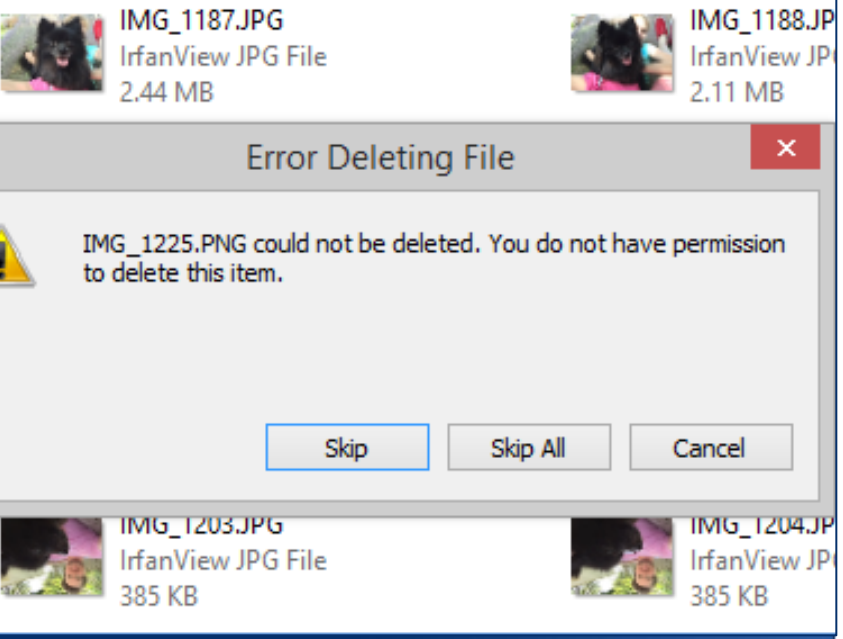
- **Otázka:** Ako by ste nastavili práva na mobile pre seba a pre deti?
  - Android (RBAC)
    - Hlavný používateľ (vlastník zariadenia) = rola s plným prístupom (všetky aplikácie, nastavenia, účty, inštalácie)
    - Hosťovský účet = dočasná rola, ktorá má prístup len k základným funkciám (telefonovanie, web, kamera), ale nie k dátam vlastníka
    - Detský profil / obmedzený používateľ = rola s výrazne obmedzenými oprávneniami – rodič vyberá, ktoré aplikácie môže dieťa používať
- **Otázka**: Je to autorizácia rolami ak ?
  - Jano (zamestnanec) sa prihlási a pokúsi sa zmazať starú faktúru => Systém mu zobrazí správu: „*Nemáte oprávnenie na mazanie súborov*.“
  - Katka (vedúca) sa prihlási a môže faktúru zmazať

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

Zhrnutie - Autorizácia na základe rolí - RBAC

- **Autorizácia na základe rolí - RBAC (Role-Based Access Control)**
  - Role v organizácii sú vopred definované
    - napr. podľa prac. pozície ako IT-čkar, Mzdár, Matrikárka, ...
  - Každá rola má svoje práva
    - Práva sa prideľujú roliam nie ľuďom
  - Osoby sa mapujú k roliam
  - **Výsledok**: Práva alebo prístup závisí od roly používateľa v organizácii
    - Príklad:
      - V nemocnici lekár (rola „lekár“) má prístup k zdravotným záznamom,
      - ale recepčná (rola „recepčná“) len k plánovaniu termínov
  - **Kde sa používa?**
    - Vo firmách, školách, úradoch – tam, kde je veľa používateľov a roly sú jasne definované
    - Rozšírená metóda autorizácie a riadenia prístupu



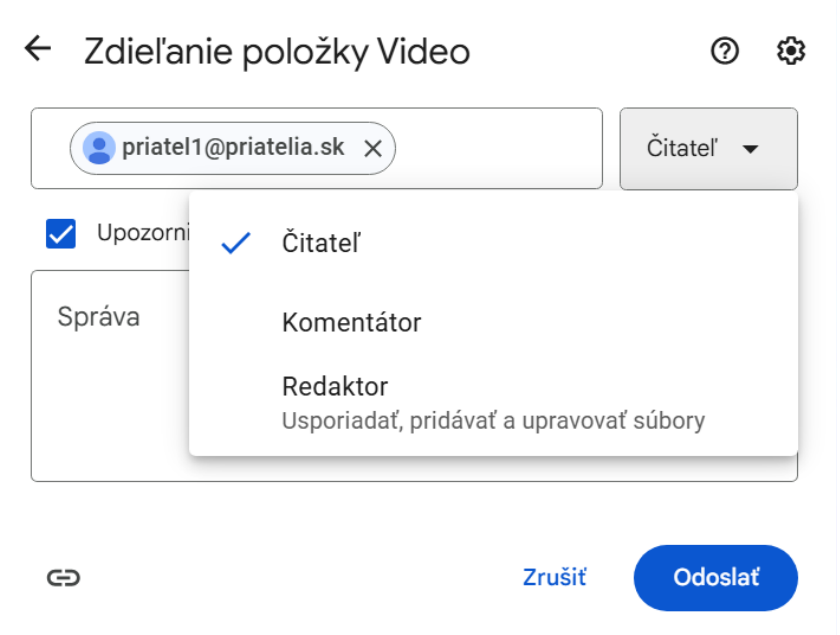


Príklad autorizácie a jej model (3.)

- **Príklad:** Používanie rodinného počítača
- **Autentifikácia**
  - Každý člen rodiny má svoj účet
  - Má možnosť prihlásiť sa do počítača
- **Autorizácia:**
  - **Mama** (vlastník priečinka s fotkami) nastavila práva:
    - **Syn**: Môže fotky pozerať, ale nemôže mazať
      - Keď to skúsi, systém mu to nedovolí
    - **Dcéra**: Môže fotky pozerať a upravovať, ale nemôže mazať.
    - **Mama**: Môže fotky upravovať aj mazať (plné práva)

Model: práva určuje vlastník – autorizácia na základe vlastníka

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



Príklad autorizácie a jej model (4.)

- **Príklad:** Používam Cloud (GoogleDrive) a chcem zdieľať priečinok s priateľmi/rodinou
- **Autentifikácia**
  - Každý sa vie prihlásiť do svojho google účtu
- **Autorizácia:**
  - **Ja (vlastník):** Mám plné práva – môžem súbory čítať, upravovať aj mazať.
  - **Priateľ 1**: Dávam mu právo len na prezeranie – môže súbory pozerať, ale nemôže ich mazať.
  - **Priateľ 2**: Dávam mu právo na úpravu – môže videá upravovať (napr. strihať), ale nemôže ich mazať.

Model: práva určuje vlastník priečinka – autorizácia na základe vlastníka

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

Zhrnutie - Autorizácia na základe vlastníka - DAC

- **Voliteľné riadenie prístupu - DAC (Discretionary Access Control)**
  - Model, kde vlastník zdroja (napr. súboru, miestnosti) rozhoduje, kto k nemu má prístup a aké práva má
    - Práva sa prideľujú objektom
    - Rozhoduje vlastník objektu
  - **Ako to funguje?**
    - Vlastník má plnú kontrolu a môže práva kedykoľvek zmeniť
  - **Kde sa používa?**
    - V menej prísnych systémoch, ako sú osobné počítače alebo malé firmy
    - Pomerne jednoduché
    - Ponúka lepšiu flexibilitu ako RBAC
    - Pre bežných používateľov najbežnejšie

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

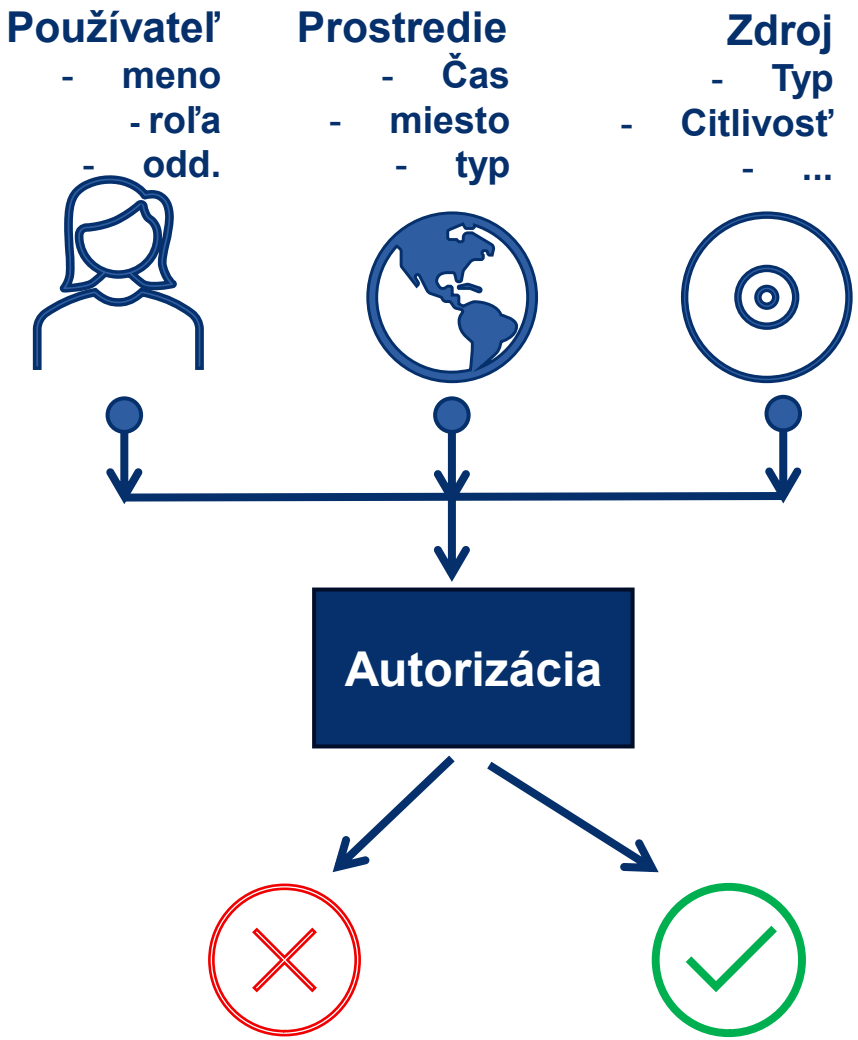
Príklad autorizácie a jej model (5.)

- **Situácia:**
  - Pracujem vo firme, ktorá používa aplikáciu na prístup k zobrazeniu faktúr podľa výšky faktúry a pracovného zaradenia
  - Prístup je riadený viacerými atribútmi, napr. používateľa, prostredia, objektu
    - Napr. Pravidlo prístupu n**a základe viacerých vlastností (atribútov)**
      - Si z daného oddelenia (napr. nižšie riadenie)? (používateľ)
      - Je pracovná doba (8:00 – 17:00)? (prostredie)
      - Ste vo firemnej sieti na svojom PC? (prostredie)
      - Je to faktúra do 5000E? (objekt)
- **Autentifikácia**
  - Prihlásim sa do systému pomocou svojho firemného e-mailu a hesla na svojom PC
- **Autorizácia**
  - Systém skontroluje moje atribúty a rozhodne, či mám povolené prezerať finančné dokumenty
    - Ak všade áno, môžem faktúru vidieť
    - Ak nie, systém mi ju nezobrazí

***Model**:* Práva prístupu určujú atribúty – autorizácia na základe atribútu

Zhrnutie - Autorizácia na základe atribútov - ABAC

- **Autorizácia na základe atribútov - ABAC (Attribute-Based Access Control)**
  - Spôsob pridelenie práv
    - Nerozhodujú len role a oprávnenia
    - Práva závisia hlavne od viacerých vlastností (atribútov)
      - **Atribúty používateľa:** napr. oddelenie (financie, HR), pozícia (manažér, zamestnanec), vek.
      - **Atribúty prostredia:** napr. čas prístupu (pracovná doba), miesto (kancelária, doma), typ siete (firemná, verejná).
      - **Atribúty zdroja:** napr. typ dokumentu (finančný, interný), úroveň citlivosti (verejné, tajné).
      - **Atribúty akcie**: napr. čítanie, úprava, mazanie.
  - Rozhodnutie o prístupe závisí od **kombinácie atribútov**
  - **Výhody:**
    - Vysoká **flexibilita**
    - **Presné** riadenie prístupu
    - Umožňuje lepšiu bezpečnosť bez nutnosti vytvárať veľké množstvo rolí



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

Príklad autorizácie a jej model (6.)

- **Situácia**:
  - Máme organizáciu ==> používa dokumenty rôznej úrovne utajenia
    - Bežné (public)
    - Dôverné (confidential)
    - Tajné (secret)
    - Prísne tajné (top secret)
  - Povolenie prístupu na základe previerky
- **Autorizácia**
  - **Príklad: Používateľ má previerku na úroveň „Dôverné“**
    - Môže čítať dokumenty označené ako „Bežné“ a „Dôverné“
    - **Nemôže** otvoriť dokumenty s označením „Tajné“ alebo „Prísne tajné“
    - **Nemôže** sám udeliť prístup inému zamestnancovi

***Model**:* Pevne a striktne určené pravidlá – model MAC

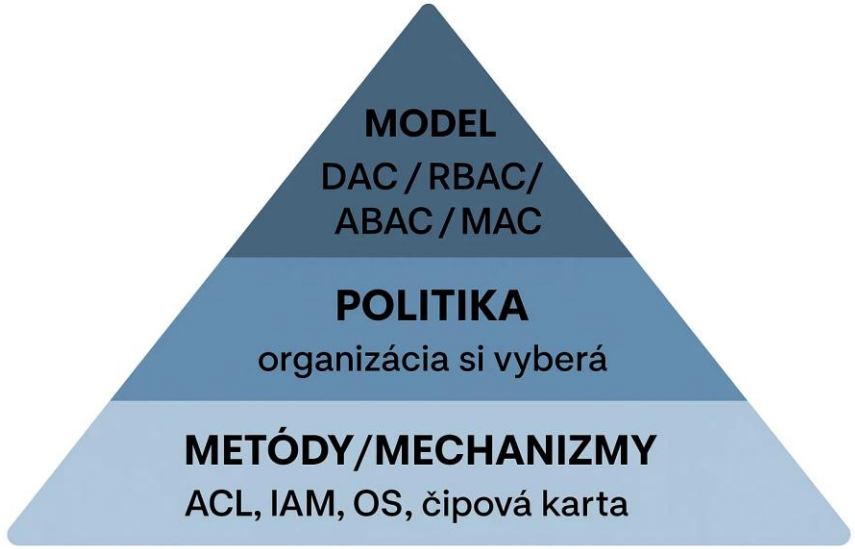
Zhrnutie – Povinné riadenie prístupu - MAC

- **Povinné riadenie prístupu - MAC (Mandatory Access Control)**
  - Prístup je kontrolovaný na základe bezpečnostných úrovní či politík
    - Často pomocou označení (napr. „tajné“, „verejné“)
  - Systém určuje pravidlá prístupu (nie vlastník alebo používateľ)
    - Podľa úrovne klasifikácie zdrojov a bezpečnostnej previerky používateľa
  - Pravidlá sú centrálne nastavené a nemenné
    - Používateľ ani vlastník si nemôže priradiť prístup alebo zdieľať dáta s niekým iným
    - Používateľ **má minimum kontroly** nad tým, ku ktorým dokumentom má prístup
  - **Ako to funguje?**
    - Prístup povolený pre zdroje ==> bezpečnostná **úroveň rovnaká alebo nižšia**
  - **Kde sa používa?**
    - V systémoch s vysokou bezpečnosťou, ako sú vládne organizácie

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

Sumarizácia - Autorizačné modely

- Príklady autorizačných metód sú:
  - RBAC (Role-Based Access Control): Prístup podľa roly
  - DAC (Discretionary Access Control): Vlastník rozhoduje o právach
  - ABAC (Attribute-Based Access Control): Prístup podľa atribútov (napr. vek, oddelenie)
  - MAC (Mandatory Access Control): Systém rozhoduje na základe bezpečnostných pravidiel



Model	Skratka	Vysvetlenie	Príklad
Discretionary Access Control	DAC	Vlastník objektu určuje, kto má aký prístup	Zdieľanie súborov v PC
Role-Based Access Control	RBAC	Práva sú viazané na **rolu** (pozíciu)	Účtovník má prístup k faktúram
Attribute-Based Access Control	ABAC	Práva sú určené na základe **atribútov** (čas, lokalita, status)	Prístup len počas pracovnej doby z určitej IP adresy
Mandatory Access Control	MAC	Bezpečnostné pravidlá	Prístup na základe previerky

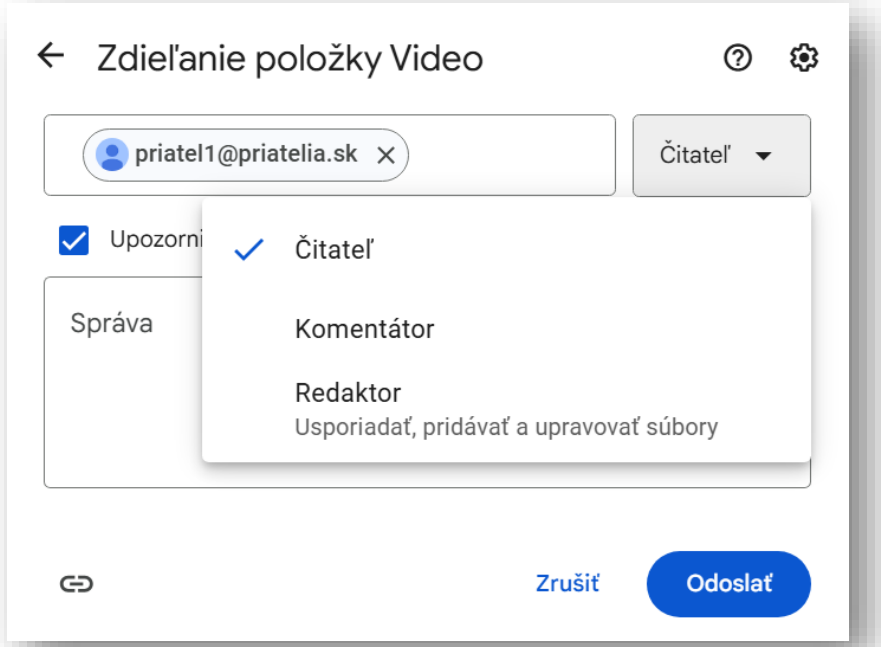
Kde sa s modelmi riadenia prístupu stretnem v bežnom živote?

- Všetky štyri modely denne využívame
  - **Asi často**
    - **DAC – Voliteľný prístup (Discretionary AC)**
      - *Život:* keď si sami rozhodujeme, kto uvidí naše súbory alebo príspevky
      - *Príklad:* zdieľanie priečinka alebo fotiek na Google Drive, nastavím „vidí/nevie upraviť“
    - **RBAC – Roly (Role-Based AC)**
      - *Život:* mobil doma – rodič má plný prístup, deti len obmedzený
      - *Príklad:* firemný počítač – zamestnanec nemôže inštalovať programy, admin áno
  - **Menej**
    - **ABAC – Atribúty (Attribute-Based AC)**
      - *Život:* online tv, alebo banková aplikácia – systém zablokuje prihlásenie z cudzej krajiny
      - *Príklad:* internet banking – prístup len počas pracovnej doby z firemnej siete
    - **MAC – Povinný prístup (Mandatory AC)**
      - *Príklad:* zdravotná karta alebo eID – len lekár so správnou previerkou uvidí dáta
      - *Život:* menej časté, ale platí v štátnej správe či banke → my ako občania to zažívame pri práci s „tajnými“ alebo oficiálnymi dokumentmi

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

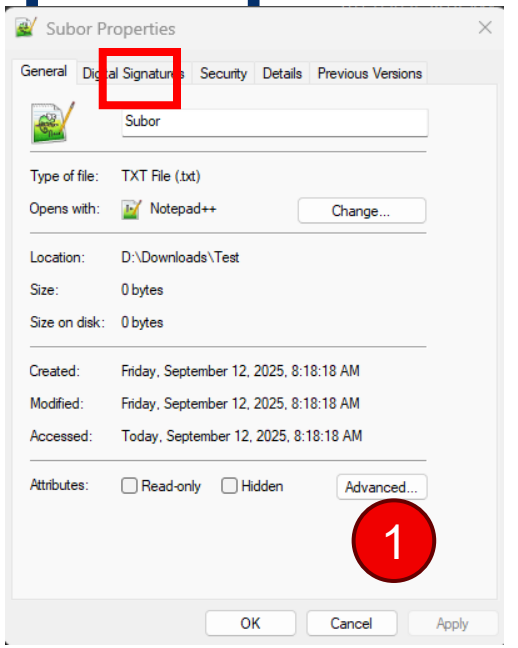
Príklad DAC: Ako nastaviť zdieľanie priečinka v Google Drive

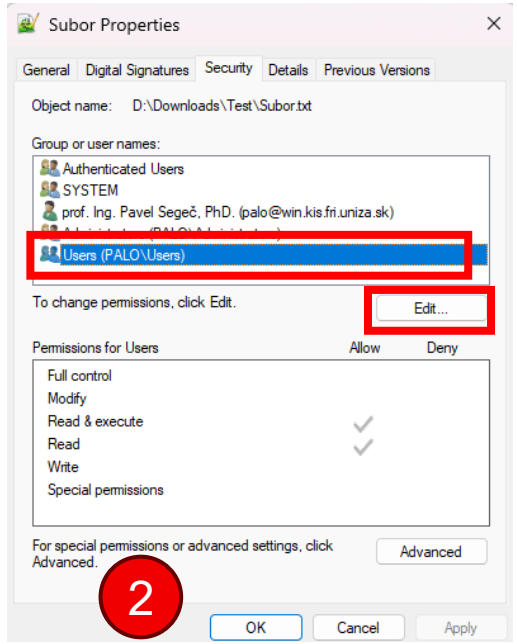
- **Prihlás sa do Google Drive**
  - otvori drive.google.com
  - prihlás sa svojím Google účtom
- **Nájdi priečinok, ktorý chceš zdieľať**
  - klikni pravým tlačidlom na názov priečinka
- **Vyber možnosť „Zdieľať“ (Share)**
  - otvorí sa okno nastavení zdieľania
- **Pridaj používateľa alebo skupinu**
  - napíš e-mailovú adresu osoby, s ktorou chceš priečinok zdieľať
  - alebo použi „Kopírovať odkaz“ a nastav, kto má k nemu prístup
- **Nastav úroveň oprávnení (DAC – ty rozhoduješ):**
  - **Čitateľ / Viewer (Len na čítanie)** → osoba môže len pozerať súbory
  - **Komentátor / Commenter (Komentovať)** → osoba môže pridávať poznámky, ale nie meniť súbory
  - **Redaktor / Editor (Upravovať)** → osoba môže pridávať, meniť alebo mazať súbory
- **Potvrď zdieľanie**
  - klikni na **Send / Hotovo**

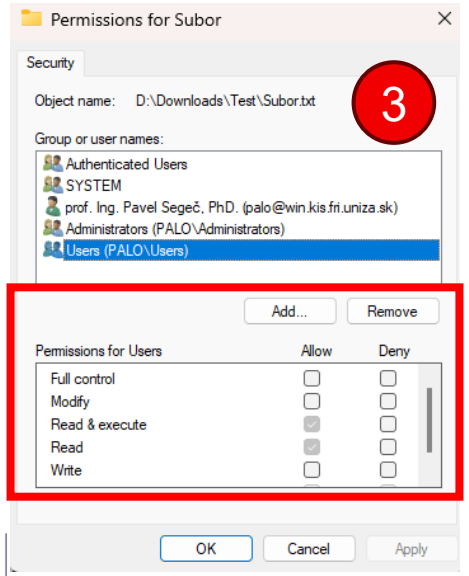


Príklad DAC: Ako nastaviť prístupové práva k súboru/priečinku vo Windows

- **Nájdi súbor alebo priečinok**
  - klikni pravým tlačidlom → **Vlastnosti (Properties)**
- **Prejdi na kartu „Zabezpečenie (Security)“**
  - tu vidíš zoznam používateľov a skupín
- **Vyber používateľa alebo skupinu**
  - napr. „Palo (local)“, „Users“, „Administrators“
- **Nastav oprávnenia:**
  - **Read (Čítanie)** – môže otvoriť súbor, ale nie meniť
  - **Write (Zápis)** – môže pridávať alebo upravovať obsah
  - **Execute (Spustiť)** – pre programy – či sa môžu spúšťať
  - **Modify (Upraviť)** – kombinácia čítania + zápisu + mazania
  - **Full Control (Plná kontrola)** – môže robiť všetko (vrátane meniť oprávnenia)
- **Potvrď zmeny → Apply / OK**







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

Systém riadenia/kontroly prístupu (Access Control)

Autentifikácia + Autorizácia = Systém riadenia prístupu

Autentizácia + **Autorizácia**

(„Kto ste?“) („Čo môžete robiť“)

- Spolupracujú a tvoria systém zabezpečenia (bezpečnostný systém)
  - Systém **Riadenia prístupu (Access Control)**
    - Centrálny prvok počítačovej (kybernetickej) bezpečnosti
    - Definuje **pravidlá a mechanizmy**, podľa ktorých rozhodujeme o overení a autorizovaní

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

Riadenie prístupu – čo je to?

- ***Kontrola prístupu*** *(Access Control)*
  - *Ponúka možnosť určovať, kto má kam prístup a čo smie robiť*
  - Je to základný bezpečnostný koncept, mechanizmus, prostriedok ...

- Reálny príklad:
  - Pri vstupe do lietadla musíme ukázať doklad totožnosti + platnú letenku.
    - ✔ Overia kto sme (autentizácia)
    - ✔ Rozhodnú, či smieme nastúpiť (autorizácia = kontrola prístupu)
- V IT svete:
  - Kontrola prístupu rozhoduje:
    - K akým súborom, aplikáciám alebo nastaveniam má používateľ prístup
    - Aké operácie môže vykonať (čítať, meniť, mazať)

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

Typy kontroly prístupu

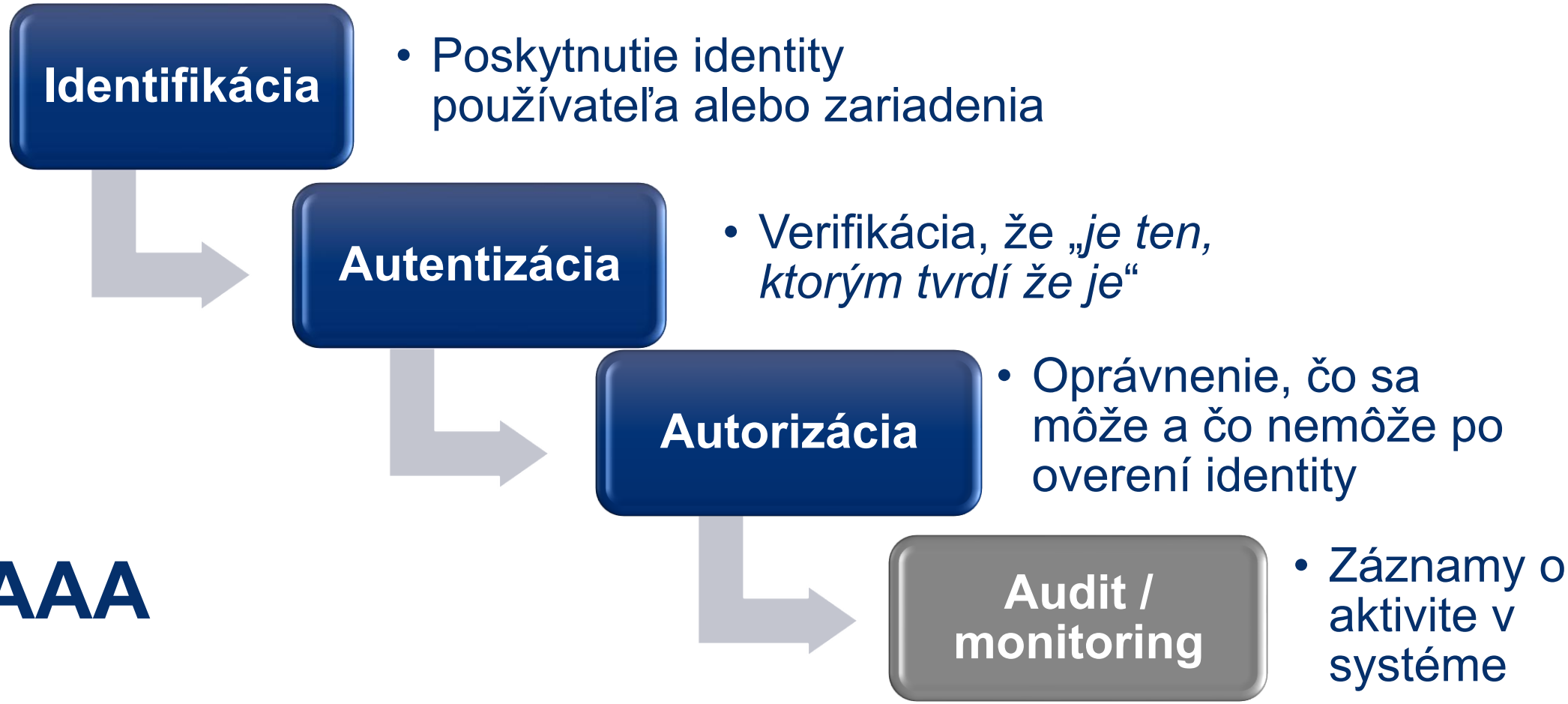
Typy kontroly prístupu (kategórie)**:**

- 🧱 **Fyzická kontrola** prístupu
  - Vstup do fyzického objektu a zabezpečenie pomocou preukazu, zámky, turnikety, kamery, ochranka, psy ....
- 💻 **Logická (technická) kontrola** prístupu
  - Heslá, smart karty, biometria,firewall
    - „IT-čko!“
- 📋 **Administratívna kontrola** prístupu
  - Politiky, školenia, prideľovanie rolí a právomocí

- Typy kontroly prístupu = spôsob vykonania (čo používame v organizácii)
  - Nástroje a opatrenia

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

Systém Riadenia prístupu (Access Management System)



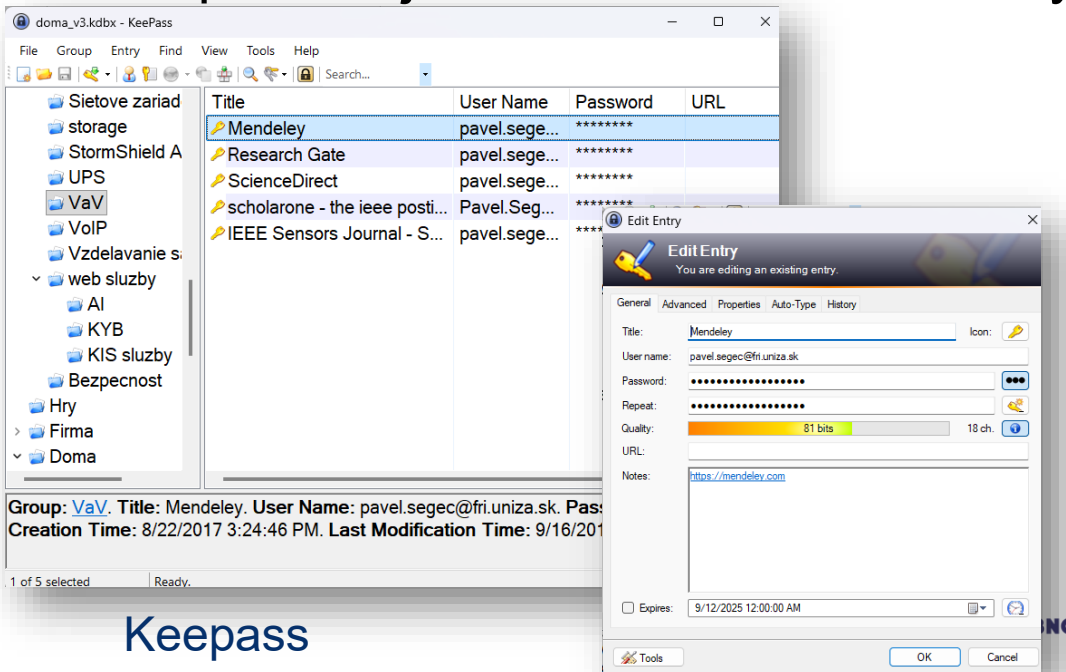
AAA

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

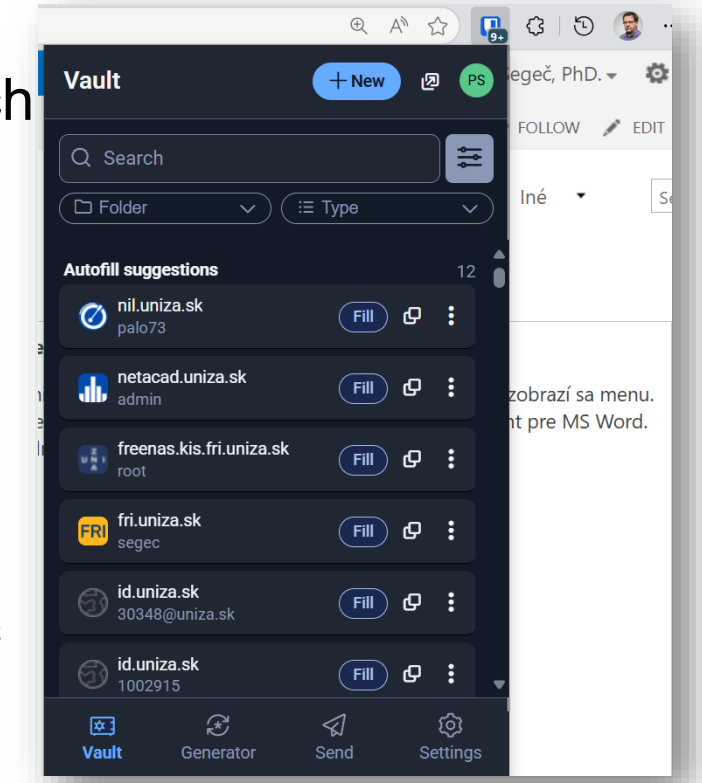
Odporúčané postpy (best practises) pre systémy autorizácie a riadenia prístupu

Odporúčania a najlepšie postupy

- **Silné heslá a ich správa**
  - Vytvorte si, používajte či vyžadujte silné, jedinečné heslá a používajte systémy na ich správu
    - Slabé heslo je ako slabý zámok na dverách – ktokoľvek ho môže ľahko prelomiť
  - Používajte správcov hesiel (napr. Bitwarden, Keepass, Google password manager) a vynucujte pravidlá (dĺžka, kombinácia znakov)
  - Nepoužívajte to isté heslo na viacerých miestach / službách



Keepass



Bitwarden web prehliadač plugin

Odporúčania a najlepšie postupy

- **Silné heslá a ich správa**
  - Vytvorte si a vyžadujte silné, jedinečné heslá a používajte systémy na ich správu
    - Slabé heslo je ako slabý zámok na dverách – ktokoľvek ho môže ľahko prelomiť
  - Používajte správcov hesiel (napr. Bitwarden, Google password manager) a vynucujte pravidlá (dĺžka, kombinácia znakov)
  - Nepoužívajte to isté heslo na viacerých miestach
- **Nikdy nepožičiavaj svoj účet ani heslo**
  - Nesieš zodpovednosť za to, čo sa pod tvojím účtom stane – aj keď to nespravíš ty
    - Zdieľanie s kolegami, rodinou alebo kamarátmi môže mať vážne následky
- **Používajte aspoň 2faktorovú autentifikáciu (Two-Factor Authentication - 2FA)**
  - Kombinujte, ak je to možné, viac spôsobov overenia identity
    - napr. heslo + kód zo SMS, alebo heslo a kód do emailu
  - Zvyšuje bezpečnosť aj v prípade, že je heslo kompromitované
    - Ak je jeden faktor kompromitovaný, druhý to môže zachrániť
  - Implementujte si 2FA/MFA pre všetky citlivé systémy a aplikácie

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

Odporúčania a najlepšie postupy

- **Riadenie prístupu na zdieľaných zariadeniach**
  - Ak používate počítač viacerí, vytvorte pre každého vlastný účet
    - Každý má svoje súbory a nastavenia, a vy rozhodnete, kto čo môže robiť
    - Vytvorte účty pre členov rodiny. administrátorské práva (napr. na inštaláciu programov) nechajte len sebe
- **Princíp najmenších privilégií (Principle of Least Privilege - POLP)**
  - Ak vytváraš role, každý používateľ alebo zariadenie by malo mať iba tie prístupové práva, ktoré sú nevyhnutné na vykonávanie jeho úloh
    - Minimalizuje riziko zneužitia privilégií a obmedzuje škody v prípade kompromitácie účtu
- **Buď opatrný pri prihlasovaní mimo pracoviska**
  - Nezadávaj svoje pracovné údaje na neznámych zariadeniach alebo cez verejné Wi-Fi
  - Ak treba, použi VPN => *bude samostastná prednáška*

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

Najlepšie postupy

- **Pravidelné kontroly prístupových rolí a práv**
  - Kontroluj, či používatelia nemajú nadbytočné práva
  - Pravidelne kontrolujte a revidujte prístupové práva, aby ste zabezpečili ich aktuálnosť a odstránili nevyužité privilégiá
- **Architektúra nulovej dôvery**
  - Ničomu nedôverujte automaticky
  - Každý prístup musí byť overený, bez ohľadu na zdroj (vnútri alebo mimo siete)
- **Oddelenie povinností**
  - Rozdeľte citlivé úlohy medzi viacerých používateľov, aby žiadny jednotlivec nemal úplnú kontrolu
    - Jeden používateľ schvaľuje transakciu, druhý ju vykoná

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

Najlepšie postupy

- **Monitorovanie a zaznamenávanie prístupu**
  - Sledujte a zaznamenávajte aktivity používateľov v systéme
- **Neboj sa pýtať a učiť sa**
  - Nemusíš byť IT expert
  - ale vedieť základy bezpečného správania online je dnes **rovnako dôležité ako vedieť čítať a písať**
- **Pravidelné školenia a zvyšovanie povedomia**
  - Vzdelávajte sa
  - či vzdelávajte používateľov o bezpečnostných postupoch a správnom používaní prístupu
  - Znižuje sa riziko chýb spôsobených nedostatočnou informovanosťou

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

Zhrnutie prednášky – Čo si zapamätať?

1. **Autentizácia vs. Autorizácia**
   - Autentizácia = Kto ste? Overenie identity (napr. heslom, otlačkom).
   - Autorizácia = Čo môžete robiť? Pridelenie prístupových práv.
2. **Prečo je autorizácia dôležitá?**
   - Chráni dáta pred zneužitím
   - Zabezpečuje kontrolu prístupu k zdrojom
   - Podporuje dôveru, súkromie a bezpečnosť
3. **Modely riadenia prístupu**
   - DAC – Vlastník určuje prístup (napr. zdieľanie súborov na Google Drive)
   - RBAC – Prístup podľa roly (napr. lekár vs. recepčná)
   - ABAC – Prístup podľa atribútov (napr. pozícia, čas, miesto, typ dokumentu)
   - MAC – Prístup podľa bezpečnostnej úrovne (napr. „tajné“, „dôverné“)
4. **Pravidlá správneho nastavenia prístupu**
   - Používaj princíp najmenších privilégií
   - Reviduj prístupové práva pravidelne
   - Využívaj viacfaktorovú autentifikáciu (2FA)
   - Sleduj a loguj prístupové udalosti

Vzorové otázky

- **Čo znamená pojem „autentizácia“?**
  - **Overenie identity používateľa**
  - Priradenie práv používateľovi
  - Zabránenie prístupu k systému
  - Vymazanie účtu používateľa

- **Princíp najmenších privilégií znamená, že:**
  - **Používateľ má len tie práva, ktoré potrebuje na svoju prácu**
  - Každý má plný prístup k systému
  - Administrátori nemajú žiadne obmedzenia
  - Používateľ si sám priraďuje oprávnenia

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
Autorizácia a riadenie prístupu

Autorizácia, monitorovanie a riešenie incidentov (Blok IV)

Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti

Pavel Segeč

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

Pavel.Segec@fri.uniza.sk