Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

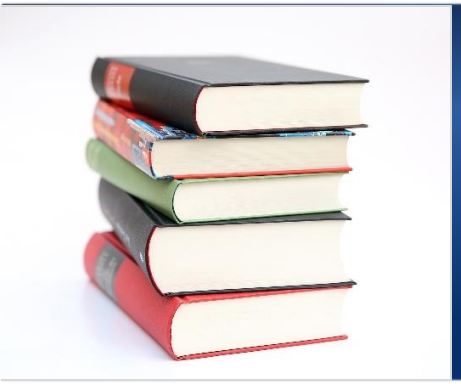
# Základné zásady (kyber)bezpečnosti pri ochrane súkromia

## Ochrana dát a súkromia (Blok VII)
Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti

Mgr. Marián Magdolen, PhD.

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

marian.magdolen@uniza.com



# Obsah

- Správna prax a bezpečnosť údajov
- Prevencia pred neoprávneným zberom a zneužitím údajov
- Ochrana osobných údajov počas online rokovaní

# Správna prax a bezpečnosť údajov

- Kybernetická bezpečnosť

- § 3 ods. 1 h)
- kybernetickou bezpečnosťou je stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje **dostupnosť, pravosť, integritu alebo dôvernosť** uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov,



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

# Správna prax a bezpečnosť údajov

- Prečo má verejná správa (ale aj jednotlivci, podnikatelia a pod.) dodržiavať kybernetickú bezpečnosť?

- Súkromie je základné ľudské právo.
- Verejná správa spracúva obrovské množstvo osobných údajov občanov.
- Únik alebo zneužitie údajov môže znamenať reálne dôsledky (od straty na životoch až po stratu dôvery a následnú právnu zodpovednosť).



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

# Správna prax a bezpečnosť údajov

- Aké sú najčastejšie hrozby?

- Phishing (podvodné e-maily).
- Malware a ransomvér.
- Neoprávnený prístup k účtom/údajom/súkromným informáciám.
- Strata alebo krádež zariadenia.
- Úniky dát.



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

# Zásady bezpečnej e-mailovej komunikácie

- Neposielať citlivé údaje nešifrované.
- V prípade šifrovania alebo zaheslovaných súborov posielať heslo iným kanálom.
- Overovať adresu príjemcu. Vyvarovať sa používaniu hromadných mailov/adresátov.
- Odpovedať vždy len oprávneným príjemcom.
- Používať oficiálne kanály (služobný e-mail).
- Pridanie informácií o súkromí a zásadách spracúvania osobných údajov do päty správ.



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

# Bezpečné prílohy a odkazy

- Otvárať súbory len z overeného zdroja.
- Posielať len nevyhnutné prílohy.
- Nepovoľovať makrá v dokumentoch.
- Prílohy určené iba na oboznámenie posielať v nemeniteľných formátoch.
- Skenovať prílohy antivírusom.



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

# Služobný vs. súkromný e-mail

- Striktné oddelenie pracovného a osobného použitia.
- Riziko strata prehľadu, náhodné zverejnenie, nedostatočné zabezpečenie.
- Monitorovanie komunikácie zamestnávateľom.
- Organizácie by mali myslieť aj na postúpenie informácií a správ pri ukončených pracovných pomeroch (Nie je dovolené sprístupňovať emailové konto iným osobám).



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

# Správa hesiel

- Využívať silné heslá
  - Minimálne 12 znakov.
  - Kombinácia veľkých/malých písmen, číslic a symbolov.
- Nepoužívať rovnaké heslo na viacerých miestach.
- Používať password manager.
- Heslá si nepamätať v prehliadači.
- Pravidelne meniť kritické heslá.
- Priebežne zisťovať, či moje heslo nie je na zozname uniknutých hesiel.



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

# Správa hesiel

- **Ako dlho trvá prelomiť heslo hrubou silou (brute-force)**
  - Ak heslo obsahuje len malé písmená (26 znaková abeceda):
    - 8 znakov → cca 22 minút
    - 10 znakov → cca 2 mesiace
    - 12 znakov → cca 12 000 rokov
  - Ak heslo obsahuje malé + veľké písmená (52 znakov):
    - 8 znakov → cca 22 hodín
    - 10 znakov → cca 5 rokov
    - 12 znakov → cca 52 000 000 rokov
  - Ak heslo obsahuje malé + veľké písmená + číslice (62 znakov):
    - 8 znakov → cca 2 dni
    - 10 znakov → cca 12 rokov
    - 12 znakov → cca 3 miliardy rokov
  - Ak heslo obsahuje malé + veľké písmená + číslice + špeciálne znaky (95 znakov):
    - 8 znakov → cca 8 hodín – 3 dni (závisí od výkonu)
    - 10 znakov → cca 100 rokov
    - 12 znakov → cca 200 000 000 rokov

# Mobilné zariadenia

- Zabezpečiť PINom alebo biometricky.
- Pravidelne aktualizovať OS a aplikácie.
- Nepoužívať verejné Wi-Fi na služobné účely.
- Zariadenia používané mimo vyhradených priestorov by mali mať šifrované úložiská.



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

# Externé pamäťové médiá

- Používať len schválené a šifrované médiá
- Nepoužívať neznáme USB („nájdené na ulici“)
- Vždy zabezpečiť heslom alebo šifrovaním citlivé údaje
- Pri prenose medzi inštitúciami využívať oficiálne kanály (nie USB)
- Po prenose dáta zmazať alebo médium bezpečne uložiť



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

# Obmedzenie digitálnej stopy

- Nastaviť cookies (iba nevyhnutné).
- Používať anonymné okno, VPN.
- Minimalizovať zdieľanie osobných údajov.
- Nastavenie súkromia účtu.
- Obmedziť viditeľnosť príspevkov.
- Nepublikovať zbytočné osobné informácie.



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

# Ochrana osobných údajov počas online rokovaní

- **Bezpečné pripojenie**
  - Používať VPN alebo služobnú sieť.
  - Vyhnúť sa verejným Wi-Fi.
  - Používať schválené softvéry na komunikáciu.

- **Nastavenie videohovorov**
  - Používať heslá na meetingy.
  - Povoliť čakáreň.
  - Kontrolovať účastníkov.



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

# Ochrana osobných údajov počas online rokovaní

- **Zdieľanie obrazovky**
  - Zavrieť citlivé dokumenty.
  - Skontrolovať pozadie a otvorené aplikácie.

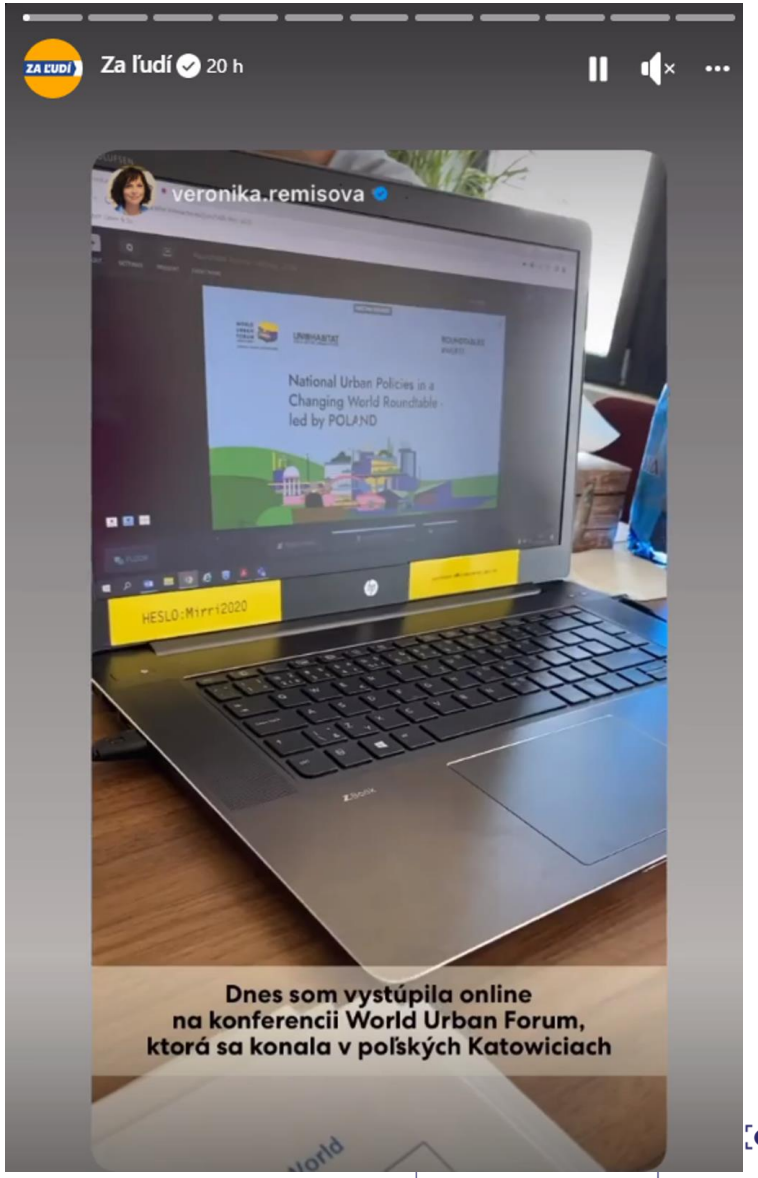
- **Prostredie a pozadie**
  - Používať virtuálne pozadie.
  - Slúchadlá = diskrétnosť.
  - Dbať na profesionálny dojem.
  - Pozor na okolie v prípade záznamu z rokovania.



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

## Základné zásady (kyber)bezpečnosti

# Ochrana osobných údajov počas online rokovaní




# Ochrana osobných údajov počas online rokovaní

- **Nahrávanie rokovaní**
  - Len so súhlasom účastníkov.
  - Záznam = osobný údaj podľa GDPR.
  - Správne uchovávanie a likvidácia.
  - Využívanie botov / AI len na základe povolenia a informovania účastníkov.



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

## Základné zásady (kyber)bezpečnosti pri ochrane súkromia

Ochrana dát a súkromia (Blok VII)

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

Mgr. Marián Magdolen, PhD.

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

marian.magdolen@uniza.sk