Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Bezpečnosť mobilných zariadení

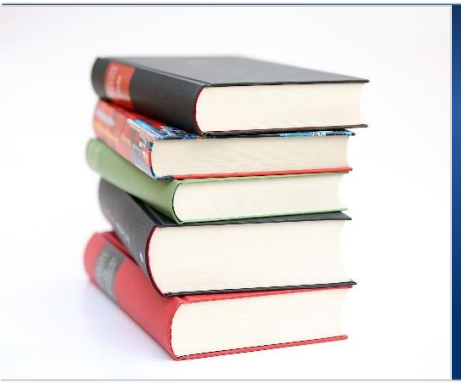
Bezpečnosť pri bezdrôtovej komunikácií, vzdialenom prístupe, využívaní cloudu a IoT zariadení (Blok VI)

Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti

Ivana Brídová

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

ivana.bridova@uniza.sk



Obsah

- Zraniteľnosti smartfónov, tabletov a bežné hrozby pre mobilné zariadenia.
- Dôležitosť aktualizácií a bezpečnostných opatrení.
- Zabezpečenie mobilných zariadení.
  - Nastavenie bezpečnostných funkcií (PIN, biometria).
  - Inštalácia a používanie bezpečnostných aplikácií.
  - Ako si overiť minimálnu dobu podpory zariadenia a prečo je to dôležité?

Mobilné zariadenia

- Mobilné zariadenia sú prenosné elektronické zariadenia, ktoré umožňujú komunikáciu, prístup na internet, prácu s aplikáciami a ukladanie dát.
- Typicky ide o: smartfóny, tablety, notebooky, inteligentné hodinky.




- **Charakteristické vlastnosti:**
  - malé rozmery a nízka hmotnosť,
  - bezdrôtová konektivita (Wi-Fi, Bluetooth, mobilné siete),
  - osobný charakter používania – uchovávajú súkromné aj pracovné informácie,
  - možnosť inštalácie aplikácií a prispôsobenia používateľovi.

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

Zraniteľnosti a možné hrozby

Zraniteľnosti smartfónov a tabletov

- **Zraniteľnosť:** je slabé miesto (chyba/nedokonalosť) v hardvéri/softvéri, alebo konfigurácií zariadenia, ktoré môže útočník použiť na získanie neoprávneného prístupu.

  - Zraniteľnosť sama o sebe nemusí znamenať útok, ale ak ju útočník nájde a zneužije, môže dôjsť k úniku dát, poškodeniu zariadenia, alebo úplnej strate kontroly nad smartfónom/tabletom.

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

Ako vyzerá zraniteľnosť mobilného zariadenia?

- **Chyba v operačnom systéme.**
- **Zle/slabé nastavenie používateľa**
  - slabý PIN (0000, 1111),
  - vypnutá šifrovacia funkcia (premieňa čitateľné dáta na nečitateľnú podobu), napr. Android používa AES (Advanced Encryption Standard),
  - povolenie inštalácie z neznámych zdrojov.
- **Zraniteľnosť hardvéru** (zber dát cez senzory).
  - Mobilné zariadenia obsahujú množstvo senzorov – napríklad mikrofón, kameru, GPS...
  - Ak sa k nim dostane útočník alebo škodlivá aplikácia, môže:
    - **odpočúvať** rozhovory cez **mikrofón**,
    - **snímať** obraz alebo okolie cez **kameru**,
    - **sledovať** polohu pomocou **GPS**,
    - dokonca **analyzovať** pohyby používateľa cez **pohybové senzory**.
    - Nebezpečenstvo spočíva v tom, že tieto senzory fungujú potichu – používateľ si často ani nevšimne, že sú zneužívané.
- **Zastaralé zariadenie** (výrobca už nevydáva bezpečnostné záplaty).

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

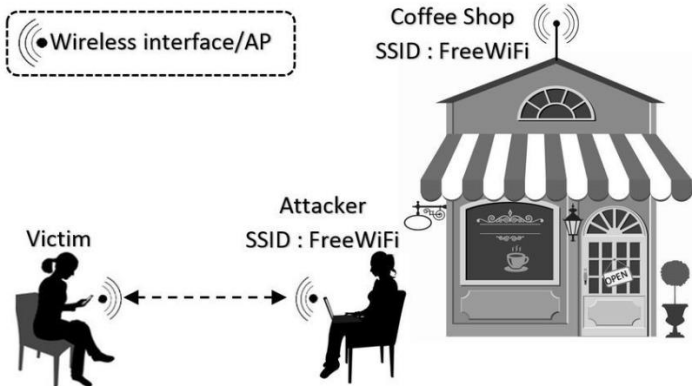
Prečo sú mobilné zariadenia terčom útokov?

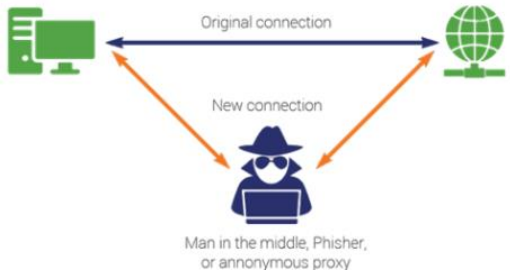
- Masívne rozšírenie zariadení - miliardy používateľov.
- Úložisko citlivých údajov - fotky, správy, bankové účty.
- Neustále pripojenie k internetu - ľahký cieľ.
- Slabé zabezpečenie zo strany používateľov.
- Rozdielna bezpečnostná podpora.

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

Príklady reálnych útokov a hrozieb

- **Malware** (škodlivý softvér). Je to program, alebo kód, ktorý je vytvorený s cieľom poškodiť PC, mobil, ukradnúť dáta alebo narušiť jeho chod. Dokáže sa šíriť cez podozrivé aplikácie.
  - **Spyware –** konkrétny typ malweru, ktorý slúži na špehovanie a zber informácií.
    - Pegasus spyware (Špehovací softvér - neviditeľné špehovanie polohy, mikrofónu, kamery a dát.)
- **Evil Twin útoky** (falošná Wi-Fi sieť s rovnakým názvom ako verejná, získava prístupové údaje cez podvrhnuté prihlasovacie stránky – riziko hlavne letiská, hotely...)
- **Man-in-the-Middle (MitM) útoky** (útočník sa vkladá medzi zariadenie a server a odchytáva dáta, heslá, prihlasovacie do účtov)
- **Phishing** (podvodný útok, zvyčajne cez e-mail, alebo webstránku. Cieľom je oklamať používateľa, aby prezradil svoje osobné údaje – heslá, číslo karty, prístupové údaje k účtom...). Útočník sa často tvári ako banka, firma...
  - **Smishing** (Podvodné SMS, e-maily, správy cez WhatsApp/Messenger. Útočník pošle SMS správu s odkazom alebo žiadosťou o osobné údaje)
- **Strata alebo krádež zariadenia** (dôsledky straty prístupu k dátam)





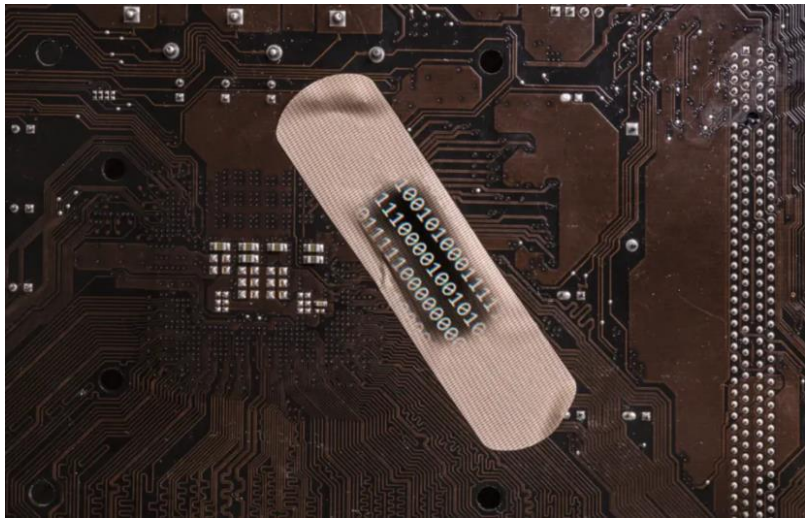
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Dôležitosť aktualizácií a bezpečnostných opatrení

Aktualizácia (update)

- **Aktualizácia** je proces, pri ktorom sa inštaluje vylepšenie alebo oprava softvéru, ktorá:
  - Zlepšuje bezpečnosť.
  - Pridáva nové funkcie.
  - Opravuje chyby a zraniteľnosti.

- **Typy aktualizácií:**
  - Aktualizácie operačného systému (OS).
  - Bezpečnostné záplaty (Security patches) – sú zamerané len na opravu zraniteľností (Android ich robí mesačne).
  - Aktualizácia aplikácií (nová verzia WhatsApp...).



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

Prečo je aktualizácia dôležitá/ako prebieha?

- Chráni pred hackermi a vírusmi, lebo opravuje chyby.
- Pridáva nové funkcie.
- Zvyšuje výkonnosť a stabilitu zariadenia.
- Zabezpečuje kompatibilitu s modernými službami a aplikáciami.

- **Ako prebieha aktualizácia?**
  - Vývojári odhalia **chybu alebo slabinu**.
  - Vytvoria **opravu** (patch) a zabalia ju do aktualizácie.
  - Používateľ si **stiahne a nainštaluje** aktualizáciu (často prebiehajú automaticky).
  - Zariadenie je po aktualizácii **bezpečnejšie a výkonnejšie**.

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

Zabezpečenie mobilných zariadení

Zabezpečenie

- Znamená súbor opatrení a technológií, ktoré chránia smartfóny, tablety a iné prenosné zariadenia pred:
  - Neoprávneným prístupom.
  - Krádežou dát.
  - Škodlivými útokmi (malware, phishing).
  - Stratou alebo zneužitím informácií.
- Ide o to, aby zariadenie aj údaje v ňom zostali v bezpečí.

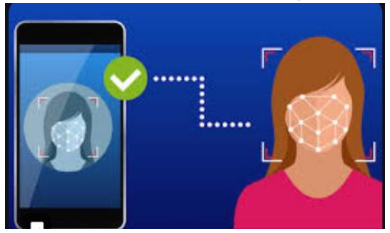
- **Prečo je zabezpečenie mobilného zariadenia dôležité?**
  - Má citlivé osobné údaje fotky, správy, heslá, banky.
  - Ak ho niekto hackne/ukradne, môže získať kontrolu na vaším digitálnym životom.
  - Dobre zabezpečenie znižuje riziko krádeže identity, podvodov a finančných strát.

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

Čo všetko zahŕňa zabezpečenie mobilných zariadení?

- **Fyzická bezpečnosť**
  - Ochrana pred stratou, alebo krádežou zariadenia.
  - Používanie PIN, hesiel, biometrie (odtlačok, FaceID) na odomknutie.






  - Automatické uzamykanie po určitej dobe nečinnosti.
  - Funkcia „Nájsť moje zariadenie“ pre vzdialená zmazanie dát.
- **Softvérová bezpečnosť**
  - Šifrovanie dát v zariadení.
  - Aktualizácia OS a aplikácií, ktoré opravujú chyby a zraniteľnosti.
  - Inštalácia aplikácií len z oficiálnych zdrojov (Google Play, App Store).

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

Bezpečnosť mobilných zariadení

- **Ochrana pred sieťovými hrozbami**
  - Nepoužívať nezabezpečené Wi-Fi siete bez VPN.
  - Vypnúť Bluetooth, NFC (Near Field Communication) keď sa nepoužívajú.
  - Používanie VPN pri práci s citlivými údajmi na verejných sieťach.

- **Ochrana dát a súkromia**
  - Dvojfaktorová autentifikácia (2FA) na účtoch (Google, Apple, banky).
  - Oprávnenia aplikácií – kontrolovať prístup k mikrofónu, kamere, polohe.
  - Zálohovanie dát do cloudových služieb (Google Drive, iCloud) – zabezpečené heslom a šifrovaním.

- **Ochrana pred škodlivým softvérom**
  - Používanie antivírusových aplikácií.
  - Blokovanie phishingových odkazov (napr. v e-mailoch alebo SMS).

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

Nastavenie bezpečnostných funkcií

- **Zámok obrazovky** (Lock Screen Security):
  - PIN kód, heslo alebo vzor (pattern) – ide o základnú ochranu pred neoprávneným prístupom.
- **Biometria:**
  - Odtlačok prsta (Fingerprint).
  - Rozpoznanie tváre (PaceID, Face Unlock).
- Nastavenie **automatického uzamknutia** po 15-30s nečinnosti.
- **Nezobrazovať citlivé notifikácie** na uzamknutej obrazovke (SMS, e-maily).
- **Dvojfaktorová autentifikácia (2FA/MFA):**
  - Aktivovať pred dôležité účty (banky, sociálne siete...).
  - Používať aplikácie na generovanie kódov (Google Authenticator, Authy) namiesto SMS.
  - Zabezpečujú, že ani pri úniku hesla sa útočník neprihlási bez druhého faktoru.

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

Bezpečnosť mobilných zariadení

- **Šifrovanie dát** (Data Encryption)
  - Väčšina nových zariadení má automaticky zapnuté šifrovanie.

- **Povolenia aplikácií**
  - Skontrolujte, ktoré aplikácie majú prístup k polohe, mikrofónu, fotoaparátu, kontaktom.
  - Odoberte povolenia, ak nie sú potrebné.
  - (Android: Nastavenia > Aplikácie > Povolenia)
  - (iOS: Nastavenia > Súkromie a zabezpečenie)

- **Sledovanie polohy a zdieľanie údajov**
  - Vypnite **GPS/polohu,** keď ju nepotrebujete.
  - Zakážte **sledovanie aktivity** aplikáciám, ktoré ho nepotrebujú.
  - (iOS: „Sledovanie aplikácií“ – povoliť/nepovoliť sledovanie)
  - (Android „História polohy“, „Zdieľanie polohy“)

Bezpečnosť mobilných zariadení

- **Automatické aktualizácie systému a aplikácií**
  - Zapnite automatické aktualizácie OS.
  - (Android: Nastavenia > Systém > Aktualizácie)
  - (iOS: Nastavenia > Všeobecné > Aktualizácia softvéru)
- Aktualizuj všetky aplikácie v Google Play/App Store.
- Opravy chýb a bezpečnostné záplaty = kľúč k ochrane.
- **Ochrana SIM karty**
  - Aktivovať PIN kód SIM karty (zabraňuje tomu, aby niekto vložil SIM do iného zariadenia a použil vaše číslo).
- Ak ste si nie istý, aké nastavenia máte aktívne, tak väčšina zariadení má **Bezpečnostnú kontrolu** alebo **Sprievodcu zabezpečením**, ktoré vás prevedie krok po kroku.

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

Minimálna doba podpory zariadení

- Ide o **časové obdobie**, počas ktorého výrobca poskytuje aktualizácie operačného systému a bezpečnostné záplaty pre konkrétne zariadenie (smartfón, tablet).

Prečo je minimálna doba podpory dôležitá?

- **Zabezpečenie**
  - Bez aktualizácií je zariadenie **zraniteľné voči útokom.**
  - Staršie zariadenia **nedostávajú záplaty** na nové zraniteľnosti.
- **Ochrana osobných údajov**
  - Telefón s neaktuálnym systémom nemusí byť schopný ochrániť vaše dáta.
  - Hackari môžu využiť staré chyby, ktoré už výrobca neopravuje.
- **Kompatibilita s aplikáciami**
  - Nové aplikácie často potrebujú novší operačný systém.
  - Bez podpory nemusia niektoré aplikácie (napr. bankové) vôbec fungovať.

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

Ako dlho výrobcovia poskytujú podporu?

- Záleží od ich aktualizačnej politiky a je potrebné si túto dobu overiť na stránke výrobcu.

Značka	Doba systémových aktualizácií	Doba bezpečnostných záplat
Apple (iOS)	5-6 rokov	6-7 rokov
Samsung (Android)	4 roky	5 rokov
Google Pixel (Android)	7 rokov (od Pixel 8)	7 rokov
Xiaomi, Oppo, Realme	2-3 roky	2-4 roky (pri vyšších modeloch)
OnePlus	4 roky	5 rokov

- **Minimálna doba podpory** zariadení je obdobie, počas ktorého výrobca poskytuje **aktualizácie, ktoré chránia vaše zariadenie pred hackermi a zabezpečujú, že funguje správne a bezpečne.** Po skončení tejto doby je čas zvážiť **výmenu zariadenia**!

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

Bezpečnosť mobilných zariadení

Bezpečnosť pri bezdrôtovej komunikácií, vzdialenom prístupe, využívaní cloudu a IoT zariadení (Blok VI)

Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti

Ivana Brídová

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

ivana.bridova@uniza.sk