Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Bezdrôtové siete a ich zabezpečenie

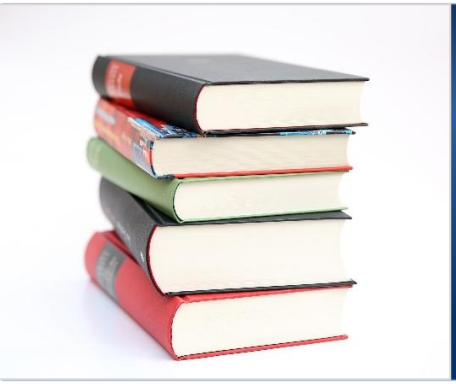
Bezpečnosť pri bezdrôtovej komunikácii, vzdialenom prístupe, využívaní cloudu a IoT zariadení (Blok VI.)

Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti vo verejnej správe

Ivana Brídová

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

ivana.bridova@uniza.sk



Obsah

- Bezdrôtová WiFi komunikácia
  - Základy fungovania WiFi sietí
  - Nastavenie a správa bezdrôtových sietí
- Hrozby pre WLAN (bežné útoky na bezdrôtové siete)
- Metódy zabezpečenia WLAN
- Bluetooth (základné bezpečnostné nastavenia)

Bezdrôtová WiFi komunikácia

Štruktúra WiFi siete

- WiFi sieť sa skladá z dvoch hlavných komponentov:

  - **Prístupový bod (Access Point, AP):**

  Ide o zariadenie (napr. WiFi router), ktoré vysiela WiFi signál a pripája iné zariadenia k internetu.

  - **Klientske zariadenia:**

  Prijímajú a odosielajú dáta cez prístupový bod (AP). Sú to zariadenia, ktoré sa dokážu k WiFi pripojiť a používať internet. (napr. telefóny, tablety, počítače, smart TV, herné konzoly, bezdrôtové tlačiarne, IoT zariadenia – smart osvetlenie, termostaty, vypínače, zásuvky, kamery)

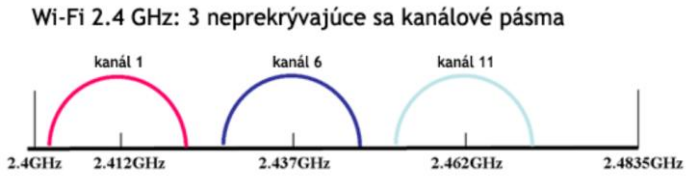
Bezdrôtová WiFi komunikácia

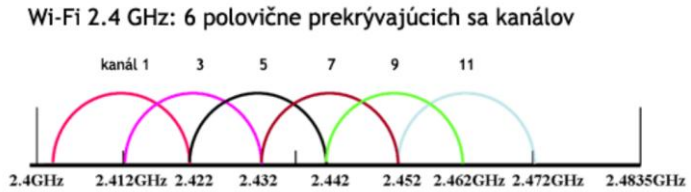
WiFi siete fungujú na princípe bezdrôtovej komunikácie pomocou rádiových vĺn, ktoré prenášajú dáta medzi zariadeniami.

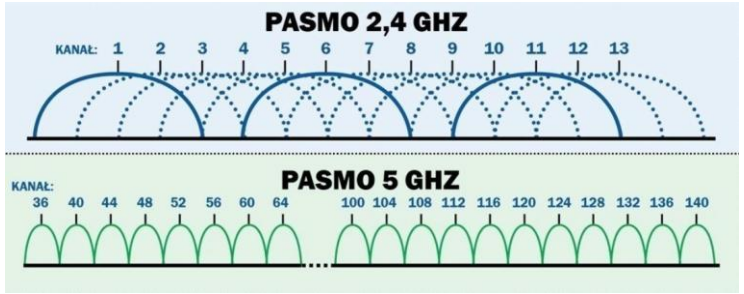
Frekvenčné pásma a štandardy:

WiFi siete používajú licenčne neviazané frekvenčné pásma:

- **2,4 GHz** – dlhší dosah, ale nižšia rýchlosť a vyššia náchylnosť na rušenie.
- **5 GHz** – vyššia rýchlosť, menej rušenia, ale kratší dosah (23 neprekrývajúcich sa kanálov).
- **6 GHz (WiFi 6E)** – ešte vyššie rýchlosti, menšie preťaženie siete.







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

Ako sa zariadenia pripájajú na WiFi?

1. **Zariadenie vyšle signál** do okolia, aby „zistilo“, aké WiFi siete sú k dispozícii.

2. **Router odpovie** a potvrdí, že je pripravený na pripojenie. (Router vysiela signál a na obrazovke telefónu sa zobrazí informácia, že sieť je dostupná na pripojenie.)

3. **Prebehne overenie hesla** – ak je správne, zariadenie dostane povolenie na pripojenie.

4. **Zariadenie a router začnú komunikovať** – výmena dát (napr. na telefóne sa načíta webstránka)

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

Hrozby pre WLAN (bežné útoky na bezdrôtové siete)

Kybernetický útočník

- Osoba, alebo skupina osôb, ktoré vykonávajú neoprávnené, škodlivé alebo podvodné aktivity s cieľom získať neoprávnený prístup k informáciám, narušiť systémy, poškodiť infraštruktúru alebo získať finančný či iný prospech.

- **Cieľom útočníkov môže byť:**
  - **Ukradnúť dáta** (osobné údaje, finančné informácie).
  - **Poškodiť alebo paralyzovať systémy a siete** (DoS/DDoS útoky).
  - **Infikovať systémy malvérom** (vírusy, ransomware).
  - **Získať neoprávnený prístup** k citlivým informáciám.
  - **Finančný zisk** (napr. cez vydieranie ransomvérom – softvér, ktorý zašifruje dáta obete, alebo mu zablokuje prístup a následne požaduje výkupné za odblokovanie).
  - **Špionáž alebo sabotáž.**

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

Najčastejšie techniky kybernetických útočníkov

- Útočný notebook
- „Zlé dvojča“
- Infikovaná počítačová sieť

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

Útočný notebook

- Najjednoduchšia forma útoku – útočníkovi stačí len notebook a cez špecializovaný softvér spustí MiTm (Man-in-the-Middle) útok.
- Útočník je medzi 2 komunikujúcimi stranami (napr. používateľ a Wifi sieť) a **tajne zachytáva, mení alebo manipuluje komunikáciu**.

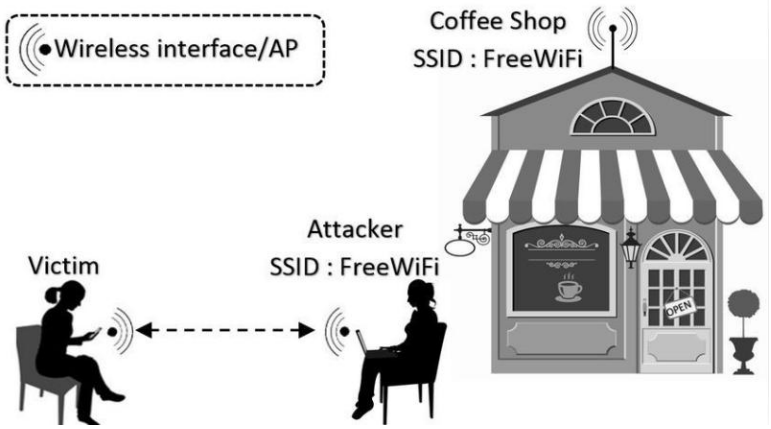
- **Princíp:**
  - Obete sa pripoja na falošný prístupový bod.
  - Útočníka odpočúva/zachytáva prenášané dáta (heslá, citlivé údaje alebo komunikáciu)
  - Môže vkladať škodlivý obsah (napr. falošné prihlasovacie formuláre).
  - Ak je slabý šifrovací protokol, môže dešifrovať aj komunikáciu.

- **Ako sa chrániť:**
  - Vyhýbať sa nebezpečným WiFi sieťam.
  - Používať VPN, ktorá šifruje komunikáciu aj pri nebezpečnej sieti.
  - Overovať certifikáty stránok HTTPS (symbol zámku v prehliadači).
  - Zapnúť firewall a aktualizovať softvér.
  - Používať viacfaktorové overenie.

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

„Zlé dvojča“ („Evil Twin AP“)

- Ide o útočníkom vytvorenú sieť, ktorá má rovnaké znaky ako iná sieť (SSID-názov siete, BSSID-MAC adresa AP, prípadne heslo).
- Signál z tejto siete má vysokú kvalitu a silu (ak sú k dispozícií 2 siete s rovnakými znakmi, tak smartfóny, notebooky, tablety a iné sa pripoja vždy k tej sieti, kde je lepší signál). V tomto prípade k falošnej.
- Aby bol útok efektívnejší, tak útočníci ešte preťažia cieľovú sieť DDoS útokom, všetkých klientov odpojí a keď sa znova pripoja, tak už sú vo falošnej sieti.

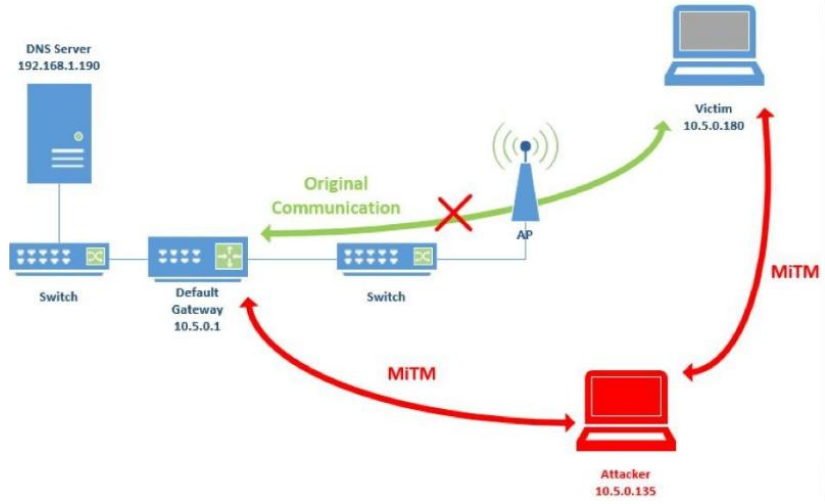


- **Ako sa chrániť:**
  - Vyhýbať sa nebezpečným WiFi sieťam.
  - Zapnúť firewall a aktualizovať softvér.
  - Používať viacfaktorové overenie.
  - Používať VPN, ktorá šifruje komunikáciu aj pri nebezpečnej sieti.
  - Overovať certifikáty stránok HTTPS (symbol zámku v prehliadači).

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

Infikovaná počítačová sieť

- Využívajú najčastejšie DoS (Denial of Service) útoky a dochádza ku softvérovej manipulácií sieťových prvkov (napr. routerov).
- „**DNSA Spoofing**“ – technika útoku, kde kópie webov kradnú heslá a čísla kariet. (Útočník vytvorí kópie stánok bánk, e-mailových služieb a iných webov. Keď sa obeť pripojí k takejto sieti a zadá adresu svojej banky, požiadavka sa zachytí a namiesto legitímneho webu sa zobrazí falošná napodobenina. Útočník následne získa všetky údaje, ktoré používateľ zadá. Odcudzené údaje sú následne zneužité, alebo predané na čiernom trhu.)
- Hlavným znakom falošného webu býva nezvyčajne dlhá URL adresa umiestnená na neobvyklej doméne. (Slovenské banky prevádzkujú svoje internetové bankovníctvo na doméne .sk. Naopak, podvodné weby sú takmer vždy prevádzkované na zahraničných doménach (.com, info, .tk, .net a podobne).)
- Naklonovaný web sa dá odhaliť len na základe chýbajúceho alebo čudného SSL/TLS certifikátu. (Je známy ako ikona zámku pri URL adrese. Pri jeho overovaní nás bude zaujímať hlavne to, pre akú inštitúciu alebo webovú lokalitu bol tento certifikát vydaný.)



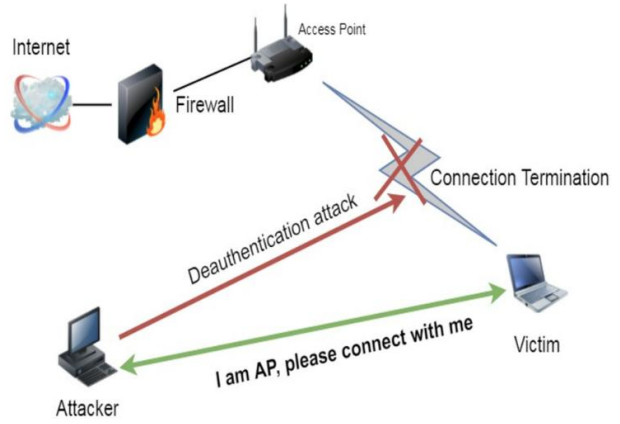
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

DoS útoky (Denial of Service)

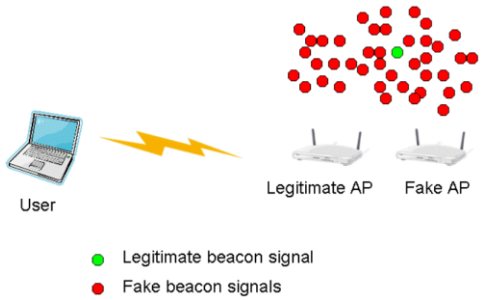
- Je typ kybernetického útoku, ktorého cieľom je narušiť, alebo znemožniť **funkčnosť bezdrôtovej siete**, alebo **pripojených zariadení**.
- Útočník sa snaží sieť preťažiť alebo zablokovať, aby používatelia nemohli využívať sieťové služby.
- Ako fungujú: útočník využíva zraniteľnosť WiFi sietí a vysiela rušivé alebo škodlivé signály, ktoré spôsobia:
  - Prerušenie spojenia.
  - Znefunkčnenie siete.
  - Odpojenie zariadení.
  - Zníženie rýchlosti alebo dostupnosti siete.

Typické metódy bezdrôtových DoS útokov

- **Rušenie signálu (Jamming):**
  - Útočník vysiela silné elektromagnetické signály na tej istej frekvencii, na ktorej funguje WiFi sieť (2,4GHz alebo 5GHz).
  - Cieľom je „prekrývať“ legitímny signál a znemožniť komunikáciu.
  - **Účinok**: Zariadenia nedokážu nadviazať, alebo udržať pripojenie k sieti.
- **Odhlasovanie zariadení (Deauthentication Attack):**
  - Útočník posiela falošné rámce, ktoré nútia zariadenia odpojiť sa od WiFi siete.
  - **Účinok**: zariadenie nedokáže nadviazať stabilné pripojenie, používateľ pociťuje neustále výpadky siete, pomalé alebo žiadne pripojenie. Sieť sa stáva prakticky nepoužiteľnou pre cieľové zariadenia.



- **Beacon Floodig** (zaplavenie oznamovacími rámcami)
  - Útočník vysiela veľké množstvo falošných oznamovacích rámcov, čím sa zahltí sieť.
  - **Účinok**: zníženie dostupností siete.



- **CTS (Clear To Send) Flooding**
  - Útočník zneužíva mechanizmus riadenia prístupu na médiu v bezdrôtových sieťach, konkrétne vysiela CTS falošné rámce. Ich opakovaným vysielaním zabezpečí, že ostatné zariadenia si myslia, že médium je stále obsadené a zariadenia prestanú komunikovať, aj keď v skutočnosti žiadny prenos neprebieha.
  - **Účinok**: používateľ neprenáša žiadne dáta cez WiFi, lebo médium sa javí ako obsadené. Ak sa útok zacieli na konkrétnu MAC adresu, dokáže ochromiť konkrétne zariadenie.

Ako môže používateľ zistiť, že prebieha DoS útok?

- **Nápadné problémy s pripojením**
  - Zariadenia často vypadávajú zo siete, aj keď je signál silný.
  - Zariadenie sa nevie pripojiť, alebo pripojenie kolíše každých pár sekúnd.
  - Pomalé načítavanie webstránok, odpájanie z online hier alebo video hovorov.

- **Zobrazovanie desiatok až stoviek Wi-Fi sietí v okolí**
  - Pri útoku typu Beacon Flooding je možné všimnúť si záplavu Wi-Fi sietí (často s čudnými názvami alebo prázdne SSID).

- **Prudké vybíjanie batérie zariadení**
  - Zariadenia sa snažia neustále pripojiť (pri deauthentication attack), čo vedie k vyššiemu odberu energie.

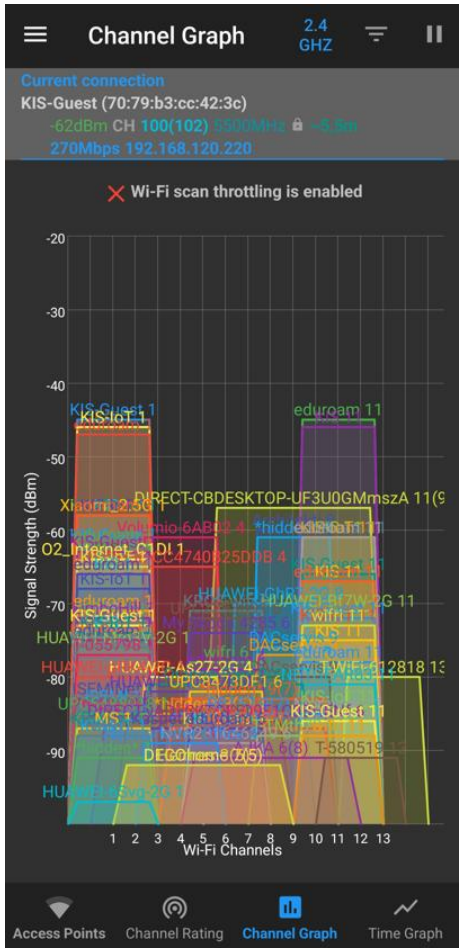
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ako bežný používateľ môže overiť útok?

```
C:\Windows\system32>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=8ms TTL=113
Reply from 8.8.8.8: bytes=32 time=8ms TTL=113
Reply from 8.8.8.8: bytes=32 time=8ms TTL=113
Reply from 8.8.8.8: bytes=32 time=8ms TTL=113

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 8ms, Average = 8ms

C:\Windows\system32>_
```

- **Ping príkaz (na overenie strát paketov a letencie)**
  - V termináli spustiť ping 8.8.8.8
  - Neustále časové výpadky, alebo žiadna odozva naznačujú problém.
- **Wi-Fi analyzer (aplikácie) môžu ukázať**:
  - Preťaženie kanálov
  - Kolízie
  - Podivné SSID alebo veľa sietí s rovnakým názvom
- **Monitoring pripojených zariadení cez router**
  - Prihlásiť sa do „admin rozhrania routera“ a skontrolovať:
    - Zoznam pripojených zariadení (MAC, IP, názov zariadenia).
    - Sleduj, či sa nepripojilo cudzie zariadenie.
    - Niektoré routre majú históriu pripojení a upozornenia.
- **Zapnúť notifikácie**, ak ich router má

(príde upozornenie, keď sa pripojí nové zariadenie).



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

Metódy zabezpečenia WLAN

Ako zabrániť útokom?

- Reštart routera a zmena Wi-Fi kanála (ak niekto ruší určitý kanál).
- Aktivovať WPA3 alebo 802.11w (Protected Management Frames), ak to AP podporuje.
- Skryt SSID. (Aj keď to nezabráni útokom, trochu to sťaží prácu útočníkovi.)
- Zmeniť heslo.
- Presunúť router alebo klienta mimo dosah útočníka. (Ak je to možné.)

Odporúčané zabezpečenie WiFi

1. **Zapnite šifrovanie** (WPA2, alternatíva WPA, ak sa nedajú zapnúť, tak aspoň WEP – jednoduché šifrovanie)
2. **Zmeňte prednastavené prístupové heslá na prístupové body a WiFi smerovače** (pôvodné heslá sú útočníkom známe a dajú sa ľahko zneužiť na prístup do siete).
3. **Zmeňte prednastavené meno siete (SSID)**
   - Útočníci poznajú prednastavené mená sietí a vyvodia si z toho, že daná sieť nie je dobre zabezpečená.
   - Nastavte si také mená, aby ich jednotlivý používatelia ľahko identifikovali, ku ktorému bodu sa chcú pripojiť.
   - Nepoužívajte mená, ktoré by boli útočníkovi veľmi nápadné (napr. OMEGA-sklad)
4. **Vypnite zdieľanie tlačiarní a súborov v sieti, ak ich nepotrebujete**
   - Týmto znemožníte prístup k údajom prípadnému útočníkovi, ktorý prelomí prístupový bod.
5. **Umiestnite prístupové body tak, aby ich signál pokrýval len územie, kde je to nevyhnutné.**
   - Niektoré prístupové body umožňujú nastaviť silu vyžarovaného signálu. Nastavte len takú, aby bolo možné pripojiť sa na ne len z bezpečnej vzdialenosti (vnútro budovy).
6. **Medzi bezdrôtovú sieť a lokálnu sieť umiestnite firewall**
   - Na ktorom povolíte len nevyhnutné služby (WEB, MAIL...).
   - Toto znemožní útočníkom prístup do siete.

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

Ako časté sú DoS útoky v bezdrôtových WiFi sieťach?

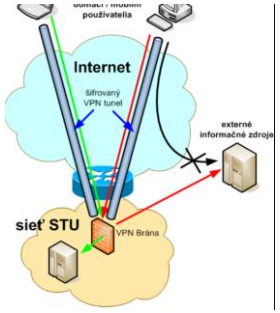
- Sú veľmi časté, veľa z nich prebieha nepretržite, lebo útočníci používajú automatizované nástroje.
- **Domáce siete – menej časté**
  - Útočníci sa zameriavajú na WiFI v prípade konkrétnej motivácie
    - Chcú získať prístup do siete.
    - Chcú spôsobiť rušenie, alebo znefunkčnenie siete.
- **Podnikové siete alebo verejné WiFi siete – častejšie**
  - Hotely, obchodné centrá, letiská – tu býva väčší pohyb ľudí, niektorí môžu útočiť na WiFi pre prístup ku klientom, alebo pre rušenie služby.
- Ak útočník cieli na konkrétnu osobu alebo sieť, tak útok môže trvať minúty až hodiny, podľa motivácie útočníka.

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

VPN (Virtual Privat Network)

FortiClient VPN
Remote Access Agent

OPENVPN



- Je technológia, ktorá dokáže z nebezpečnej siete urobiť bezpečné internetové útočisko.
- VPN vytvorí tunel medzi zariadením a cieľovým webom. Celá dátová komunikácia je tu riadne zašifrovaná a pre útočníkov nedosiahnuteľná.
- Keby ste aj boli napojený k infiltrovanej Wi-Fi siete a využijete v nej VPN, tak vaše údaje ostanú v bezpečí.
- PC z rôznych častí sveta sa dajú prostredníctvom VPN spojiť tak, akoby boli pripojené do jednej fyzickej lokálnej siete. VPN vytvorí izolovanú virtuálnu dátovú linku.

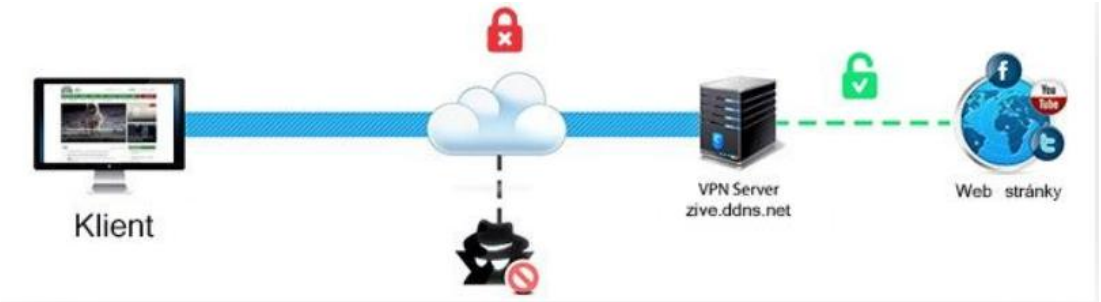
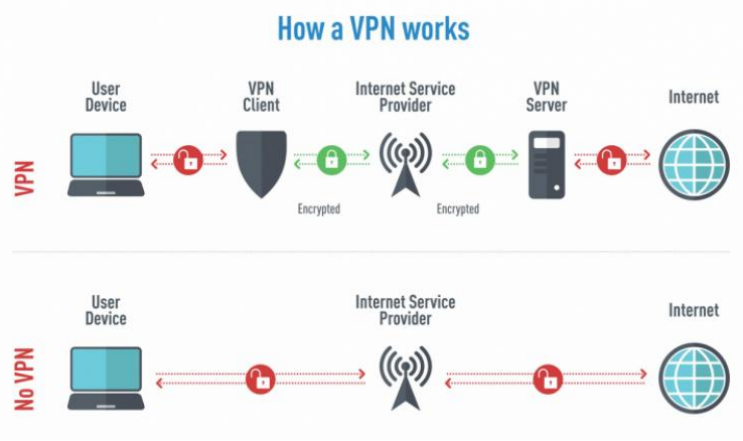


Schéma VPN tunelu.



Bluetooth

Bluetooth – čo to je?

- **Bezdrôtová komunikačná technológia na krátke vzdialenosti**, ktorá umožňuje prenos dát medzi dvoma alebo viacerými zariadeniami bez použitia kábla.
- **Funguje na rádiovej frekvencii v pásme 2,4 GHz.**
- **Je navrhnutý tak, aby:**
  - Prepojil zariadenia v blízkom okolí (cca 10 metrov, max.100 metrov, závisí od zariadenia a verzie).
  - Prenášal dáta (napr. ovládanie slúchadiel, myš, klávesnica, herné ovládače, smart hodinky, hrudné pásy, cyklopočítače...).

Verzie Bluetooth

- Bluetooth 1.0-2.0 – nízke rýchlosti, spojí len pár zariadení.
- Bluetooth 3.0-4.0 – vyššia rýchlosť. BLE (Bluetooth Low Energy) pre senzory s nízkou spotrebou energie.
- Bluetooth 5.0 a vyššie:
  - Väčší dosah (až 100 m).
  - Lepšia rýchlosť prenosu.
  - Podpora viacerých zariadení naraz.
  - Efektívnejšie pripojenie pre IoT zariadenia.

Výhody/Nevýhody Bluetooth

- **Výhody:**
  - Bezdrôtové spojenie bez internetu alebo siete.
  - Nízka spotreba energie.
  - Lacné a dostupné zariadenia.
  - Jednoduché párovanie.

- **Nevýhody:**
  - Obmedzený dosah.
  - Nižšia prenosová rýchlosť oproti Wi-Fi.
  - Potenciálne bezpečnostné riziká (ak nie je dobre zabezpečené párovanie).
  - Možnosť rušenia (lebo používa frekvenciu 2,4GHz, kde beží aj WiFi, mikrovlnky...).

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

Bezpečnosť Bluetooth

- Novšie verzie majú vylepšené **šifrovaciu komunikáciu**.
- Pri párovaní sa používa **autentifikácia** (PIN, potvrdenie).
- BLE (Bluetooth Low Energy) zariadenia často využívajú **ochranou proti sledovaniu**.
- Odporúča sa **vypínať** Bluetooth, keď sa nepoužíva.

Bezpečnosť v mobilných sieťach

- Zárukou bezpečnosti je vlastný mobilný internet.
- Ak nie je dostupný a potrebujete sa pripojiť k verejnej Wi-Fi sieti, využite radšej VPN.

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

Bezdrôtové siete a ich zabezpečenie

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

Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti vo verejnej správe

Ivana Brídová

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

ivana.bridova@uniza.sk