Andrija Lažeta, 4.D

Zaštita bežičnih mreža

Kratak sadržaj:
Bežične mreže postale su ključni dio modernog načina života, omogućujući brzi prijenos podataka i povezanost u svim aspektima svakodnevnog života. Međutim, s velikim prednostima dolaze i problem sa sigurnosti. Ovaj rad bavi se različitim načinima zaštite bežičnih mreža. Obradit će se najčešće prijetnje, preporučene sigurnosne mjere i alati za zaštitu bežičnih mreža.

Uvod

Bežične mreže omogućuju komunikaciju bez fizičkih žica i kabelskih veza, čime se olakšava pristup internetu i povezanost između uređaja. Ipak, zbog svoje prirode, bežične mreže često su izložene raznim sigurnosnim prijetnjama, uključujući neovlašteni pristup, hakiranje i krađu podataka. U ovom radu istražuju se najvažniji izazovi u zaštiti bežičnih mreža te pružaju konkretni savjeti i preporuke za osiguranje privatnosti i integriteta podataka.

Sigurnosni izazovi bežičnih mreža

Najveći sigurnosni izazovi s kojima se susreću bežične mreže uključuju:

1. **Neovlašteni pristup** – Jedan od najvećih problema je omogućavanje pristupa mreži od strane neovlaštenih korisnika, što može dovesti do krađe podataka ili zlonamjernih aktivnosti.
2. **Zlonamjerni softver i napadi** – Bežične mreže mogu biti cilj napada poput DDoS napada, sniffing-a (presretanje podataka) ili pokušaja instaliranja zlonamjernih softverskih alata koji ometaju rad mreže.
3. **Slaba enkripcija** – Mnoge mreže koriste slabe ili zastarjele enkripcijske protokole, što može omogućiti napadačima da lako dešifriraju podatke.

Mjere zaštite bežičnih mreža

Za učinkovitu zaštitu bežičnih mreža potrebno je implementirati različite sigurnosne mjere:

1. **Korištenje jakih enkripcijskih protokola** – Najvažnija mjera zaštite je korištenje jakih enkripcijskih protokola kao što su WPA3, koji nudi bolju sigurnost od starijih WPA i WEP protokola.
2. **Primjena sigurnih lozinki** – Mreža treba biti zaštićena jakim lozinkama koje uključuju kombinaciju slova, brojeva i simbola. Redovito mijenjanje lozinki također je dobra praksa.
3. **Korištenje virtualnih privatnih mreža (VPN)** – VPN omogućuje šifriranje podataka prilikom prijenosa, čime se smanjuje mogućnost presretanja podataka.
4. **Redovita ažuriranja firmware-a i softverskih aplikacija** – Ažuriranje svih mrežnih uređaja (usmjerivača, pristupnih točaka) može pomoći u popravljanju sigurnosnih rupa koje bi napadači mogli iskoristiti.
5. **Fizička zaštita uređaja** – Ovdje se misli na fizičku sigurnost pristupnih točaka, usmjerivača i drugih uređaja koji se koriste u bežičnim mrežama, kako bi se spriječila njihova krađa ili neovlašteni pristup.

Preporučeni alati za zaštitu bežičnih mreža

Postoji nekoliko alata koji mogu pomoći u osiguravanju bežičnih mreža:

1. **Wi-Fi Analyzer** – Ovaj alat omogućuje analizu bežičnih mreža u okolini, pomažući u prepoznavanju slabih točaka u zaštiti i optimizaciji signala.
2. **Aircrack-ng** – Službeni alat za testiranje sigurnosti bežičnih mreža. Iako je često korišten za hakiranje, također može pomoći u prepoznavanju slabosti u vlastitim mrežama.
3. **Firewall i antivirusni softver** – Ovi alati pomažu u zaštiti od neželjenog prometa i napada koji mogu doći s bežičnih mreža.

Zaključak

Zaštita bežičnih mreža postaje sve važnija kako se sve više uređaja povezuje na internet. Implementacija odgovarajućih sigurnosnih mjera, kao što su korištenje jakih enkripcijskih protokola, sigurnih lozinki, VPN-a i drugih alata, ključna je za očuvanje privatnosti i integriteta podataka korisnika. Redovito ažuriranje uređaja i pažljivo upravljanje pristupom mogu značajno smanjiti rizik od napada i drugih sigurnosnih prijetnji.

Izvori:

https://en.wikipedia.org/wiki/Wireless_security

Andrija Lažeta, 4.D

https://www.nist.gov/cybersecurity