Sigurnost bežičnih mreža – kako zaštititi svoju Wi-Fi vezu

Ime i prezime: Luka Perić

Razred: 3.A

Predmet: Računalne mreže

Datum: 1. lipnja 2025.

Sažetak

U današnje vrijeme gotovo svako kućanstvo koristi bežične mreže za pristup internetu, no malo tko razmišlja o sigurnosti te mreže. U ovom radu obrađujemo najčešće sigurnosne prijetnje u bežičnim mrežama, načine zaštite, protokole enkripcije poput WPA2 i WPA3 te korisne savjete kako se zaštititi. Također donosimo nekoliko primjera stvarnih napada kako bismo naglasili važnost informiranosti i edukacije korisnika, s ciljem jačanja digitalne sigurnosti u svakodnevnom životu.

Uvod

Bežične mreže su postale neizostavan dio svakodnevice. Gotovo svaki pametni telefon, laptop, televizor ili igraća konzola danas koristi Wi-Fi za pristup internetu. No, za razliku od ožičenih veza, bežične mreže su otvorene za sve u njihovom dosegu. To znači da napadač ne mora fizički ući u vaš dom kako bi pristupio vašoj mreži – dovoljno je da se nalazi unutar dometa signala. Zbog toga je ključno razumjeti kako funkcionira sigurnost bežične mreže i koje su metode za njezinu zaštitu. Pitanje sigurnosti više nije rezervirano samo za velike tvrtke – ono se tiče svakog pojedinca koji koristi internet, posebno u vlastitom domu.

Razrada

Najčešće prijetnje

Bežične mreže mogu biti ranjive iz više razloga. Najčešće prijetnje uključuju:
- Otvorene mreže bez lozinke, koje omogućuju svakome u blizini pristup internetu i mrežnim uređajima.
- Slabe lozinke koje se lako mogu pogoditi ili probiti brute-force napadom.
- Zastarjeli sigurnosni protokoli poput WEP-a, koji više ne pružaju dovoljnu razinu zaštite.
- Nepromijenjene tvorničke postavke routera koje hakeri lako mogu iskoristiti.

Vrste sigurnosnih protokola

Za zaštitu Wi-Fi mreža koriste se različiti protokoli enkripcije. WEP (Wired Equivalent Privacy) bio je prvi standard, ali se danas smatra potpuno nesigurnim. WPA (Wi-Fi Protected Access) predstavlja napredak, no još uvijek je ranjiv na određene vrste napada. WPA2 je najraširenij sigurnosni protokol koji koristi snažnu AES enkripciju i preporučuje se za većinu kućnih i poslovnih mreža. Najnoviji standard, WPA3, dodatno štiti korisnike od napada pogađanja lozinki te omogućuje sigurnije povezivanje uređaja, čak i bez zaslona, kao što su pametni kućni uređaji.

Metode zaštite mreže

Postoji niz metoda kojima možemo zaštititi svoju bežičnu mrežu. Prvo, važno je koristiti jake i složene lozinke koje sadrže kombinaciju slova, brojeva i simbola. U postavkama routera treba uključiti WPA2 ili WPA3 enkripciju, a WPS funkciju (Wi-Fi Protected Setup) treba isključiti jer predstavlja sigurnosni rizik. MAC filtracija omogućuje odobravanje pristupa samo određenim uređajima, a redovito ažuriranje firmware-a osigurava da router ima najnovije sigurnosne zakrpe. Također se preporučuje promijeniti naziv mreže (SSID) u nešto neutralno kako bi se otežala identifikacija mreže.

Primjeri napada

Među poznatijim napadima na bežične mreže nalazi se deauthentication napad, kod kojeg napadač prisilno prekida vezu između korisnika i routera. Tada pokušava uhvatiti podatke pri ponovnom spajanju. Sniffing je metoda kojom se prisluškuje mrežni promet, posebno na nezaštićenim mrežama. Evil Twin napad podrazumijeva stvaranje mreže s istim imenom kao legitimna mreža, čime korisnik nehotice pristupa lažnoj mreži, dajući napadaču pristup podacima. Ovi primjeri pokazuju koliko lako hakeri mogu zloupotrijebiti nesigurne mreže i koliko je važno djelovati preventivno.

Zaključak

Sigurnost bežičnih mreža je važnija nego ikad prije. U svijetu u kojem sve više uređaja komunicira bežično, čak i najmanja ranjivost može imati ozbiljne posljedice. Korisnici moraju biti educirani, svjesni rizika i spremni primijeniti osnovne mjere zaštite. Korištenje modernih protokola enkripcije, složenih lozinki, deaktivacija nesigurnih opcija i redovito održavanje mrežne opreme ključni su koraci prema sigurnijem digitalnom okruženju. Iako potpuna zaštita ne postoji, odgovorno ponašanje može značajno smanjiti rizike. Sigurnost ne ovisi samo o tehnologiji, već i o ponašanju korisnika.

Izvori

- https://www.wi-fi.org
- https://www.hrvatskitelekom.hr
- https://www.lifewire.com
- https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access