Sigurnost Bežičnih Mreža

UVOD

U današnjem digitalnom dobu, bežične mreže su postale neizostavan dio našeg svakodnevnog života. Omogućuju nam pristup internetu u različitim okruženjima, bilo da smo u kafićima, na aerodromima ili u udobnosti vlastitog doma. Međutim, s tom slobodom dolazi i povećani rizik od sigurnosnih prijetnji. Bežične mreže su podložne različitim vrstama napada, što može dovesti do krađe osobnih podataka, financijske štete ili čak identitetske prijevare.

SIGURNOSNI IZAZOVI BEŽIČNIH MREŽA

Bežične mreže su podložne raznovrsnim sigurnosnim prijetnjama zbog svoje inherentne prirode komunikacije putem zračnog medija. Kako bi se razumjeli ti izazovi, važno je istaknuti nekoliko ključnih napada koji su česti u bežičnim okolinama.

Napadi poput „man-in-the-middle“ (MITM) predstavljaju ozbiljnu prijetnju jer omogućuju napadačima da se ubace između dvije legitimne komunikacijske strane, čime mogu presresti i manipulirati podacima. Ovaj oblik napada može biti iznimno opasan jer korisnici često nisu svjesni da je njihova komunikacija kompromitirana.

„Evil twin“ napadi su još jedna vrsta prijetnje u kojoj se stvara lažna pristupna točka koja imitira legitimnu mrežu, često s istim nazivom (SSID) kako bi zavarala korisnike. Kada se korisnici povežu s ovom lažnom mrežom, njihovi podaci postaju dostupni napadačima.

METODE ZAŠTITE

Kao odgovor na ove izazove, korisnici mogu primijeniti niz tehnika i praksi kako bi zaštitili svoje bežične mreže.

Korištenje napredne enkripcije poput WPA2 ili WPA3 ključno je za osiguravanje da su podaci koji se prenose preko mreže zaštićeni i nečitljivi neovlaštenim stranama. Osim

toga, redovito mijenjanje lozinki, posebno nakon što gosti koriste mrežu, pruža dodatni sloj sigurnosti.

Implementacija virtualnih privatnih mreža (VPN) može dodatno poboljšati sigurnost, posebno prilikom korištenja javnih Wi-Fi mreža, omogućujući šifrirani tunel za komunikaciju između uređaja i interneta.

NAPREDNI SIGURNOSNI ASPEKTI

Pored osnovnih metoda zaštite, postoje i napredne sigurnosne tehnike koje korisnici mogu primijeniti kako bi dodatno osigurali svoje bežične mreže.

Jedna od tih tehnika je implementacija višestrukih faktora autentifikacije (MFA), koja zahtijeva više od jednog oblika autentifikacije, kao što su lozinka i biometrijski podaci, prije nego što se korisniku odobri pristup mreži. Ovo značajno otežava napadačima neovlašteni pristup čak i ako uspiju presresti ili dešifrirati lozinku.

PRIMJENA U POSLOVNOM OKRUŽENJU

U poslovnim okruženjima, gdje su osjetljivi podaci često na meti, sigurnost bežičnih mreža ima poseban značaj.

Organizacije često primjenjuju dodatne sigurnosne mjere kao što su segmentacija mreže, što ograničava pristup određenim dijelovima mreže samo na autorizirane korisnike, te stroge politike autentifikacije kako bi zaštitile osjetljive informacije od vanjskih prijetnji.

BUDUĆNOST SIGURNOSTI BEŽIČNIH MREŽA

Ubrzani razvoj tehnologije otvara put za nove izazove u sigurnosti bežičnih mreža, ali isto tako nudi i nove mogućnosti za jačanje sigurnosti.

Primjena tehnologija poput umjetne inteligencije (AI) i strojnog učenja (ML) mogu poboljšati detekciju i obranu od napada tako što omogućuju sustavima da nauče prepoznati i reagirati na nove prijetnje u stvarnom vremenu.

Uz ubrzani razvoj tehnologije, važno je naglasiti važnost kontinuiranog istraživanja i inovacija u području sigurnosti bežičnih mreža. Primjena blockchain tehnologije, na

primjer, može pružiti dodatnu sigurnost identiteta i transakcija unutar bežičnih mreža putem distribuirane i neizbrisive evidencije.

Također, važno je razvijati standarde i regulative koje promiču visoke standarde sigurnosti u industriji bežičnih mreža, osiguravajući da proizvođači i pružatelji usluga primjenjuju najbolje prakse u zaštiti korisničkih podataka i privatnosti.

Kroz suradnju između svih dionika, od korisnika i tvrtki do istraživačkih institucija i vlada, možemo stvoriti održivo i sigurno okruženje za bežične komunikacije u budućnosti

ZAKLJUČAK

Sigurnost bežičnih mreža postaje sve važnija kako se sve više oslanjamo na njih u svakodnevnom životu. Kombinacija osnovnih i naprednih sigurnosnih tehnika, zajedno s edukacijom korisnika i suradnjom među industrijom, ključna je za očuvanje integriteta bežičnih mreža u budućnosti.

Poveznice:

https://mario-kopjar.from.hr/racunalne-mreze/wifi-security/

https://zir.nsk.hr/islandora/object/algebra:525/datastream/PDF/download

https://www.cis.hr/sigurnosni-alati/ispitivanje-sigurnosti-bezicnih-mreza.html

https://repozitorij.unipu.hr/islandora/object/unipu:180/datastream/PDF/view

https://repozitorij.algebra.hr/islandora/object/algebra:525/datastream/PDF/download