Zaštita bežičnih mreža

U današnjem povezanom svijetu gotovo svatko ima barem jedan uređaj povezan s internetom. Budući da je broj ovih uređaja u porastu, važno je implementirati sigurnosnu strategiju kako bi se smanjio njihov potencijal za iskorištavanje (pogledajte Osiguranje interneta stvari). Uređaje povezane s internetom mogu zlobni entiteti koristiti za prikupljanje osobnih podataka, krađu identiteta, kompromitiranje financijskih podataka i tiho slušanje—ili gledanje—korisnika. Poduzimanje nekoliko mjera opreza pri konfiguraciji i korištenju vaših uređaja može spriječiti ovu vrstu aktivnosti.

Koji su rizici za vašu bežičnu mrežu?

Bez obzira radi li se o kućnoj ili poslovnoj mreži, rizici za nezaštićenu bežičnu mrežu su isti. Neki od rizika uključuju:

Piggybacking

Ako ne uspijete osigurati svoju bežičnu mrežu, svatko s računalom s omogućenom bežičnom mrežom u dometu vaše pristupne točke može koristiti vašu vezu. Tipični domet pristupne točke u zatvorenom prostoru je 45-90 metara. Na otvorenom, ovaj raspon može se protezati do 300 metara. Dakle, ako je vaše susjedstvo usko naseljeno, ili ako živite u stanu ili stambenoj zgradi, neuspjeh da osigurate svoju bežičnu mrežu mogao bi otvoriti vašu internetsku vezu mnogim nenamjernim korisnicima. Ovi korisnici mogu obavljati nezakonite aktivnosti, nadzirati i hvatati vaš web promet ili ukrasti osobne datoteke.

Wardriving

Wardriving je specifična vrsta piggybackinga. Domet emitiranja bežične pristupne točke može učiniti internetske veze dostupnima izvan vašeg doma, čak i na vašoj ulici. Pametni korisnici računala to znaju, a neki su napravili hobi od vožnje kroz gradove i četvrti s računalom opremljenim bežičnom vezom—ponekad sa snažnom antenom—tražeći nezaštićene bežične mreže. Ova praksa je poznata kao “wardriving”.

Evil Twinning

Neovlaštena osoba prikuplja informacije o pristupnoj točki javne mreže, a zatim postavlja svoj sustav da je oponaša. Protivnik koristi emitirani signal jači od onog koji generira legitimna pristupna točka; tada se korisnici koji ništa ne sumnjaju povezuju koristeći jači signal. Budući da se žrtva spaja na internet putem napadačevog sustava, napadaču je lako koristiti specijalizirane alate za čitanje svih podataka koje žrtva šalje putem interneta. Ovi podaci mogu uključivati brojeve kreditnih kartica, kombinacije korisničkog imena i lozinke i druge osobne podatke. Prije upotrebe uvijek potvrdite ime i lozinku javne Wi-Fi pristupne točke. Ovo će osigurati da se povezujete na pouzdanu pristupnu točku.

Wireless Sniffing

Mnoge javne pristupne točke nisu osigurane i promet koji nose nije šifriran. To može ugroziti vašu osjetljivu komunikaciju ili transakcije. Budući da se vaša veza prenosi “jasno”, zlonamjerni hakeri mogu koristiti alate za njuškanje kako bi dobili osjetljive informacije poput lozinki ili brojeva kreditnih kartica. Provjerite koriste li sve pristupne točke na koje se povezujete najmanje WPA2 enkripciju.

Neovlašteni pristup računalu

Neosigurana javna bežična mreža u kombinaciji s nezaštićenim dijeljenjem datoteka mogla bi zlonamjernom korisniku omogućiti pristup svim direktorijima i datotekama koje ste nenamjerno učinili dostupnima za dijeljenje. Osigurajte da kada povezujete svoje uređaje s javnim mrežama, zabranite dijeljenje datoteka i mapa. Dopustite samo dijeljenje na prepoznatim kućnim mrežama i samo dok je potrebno dijeliti stavke. Ako nije potrebno, provjerite je li dijeljenje datoteka onemogućeno. To će spriječiti nepoznatog napadača da pristupi datotekama vašeg uređaja.

Shoulder Surfing

Na javnim mjestima zlonamjerni akteri mogu jednostavno baciti pogled preko vašeg ramena dok tipkate. Jednostavno vas promatrajući, mogu ukrasti osjetljive ili osobne podatke. Zaštitne folije koje onemogućuju surferima da vide zaslon vašeg uređaja mogu se kupiti za malo novca. Za manje uređaje, kao što su telefoni, budite svjesni svoje okoline dok gledate osjetljive informacije ili unosite zaporke.

Krađa mobilnih uređaja

Ne oslanjaju se svi napadači na dobivanje pristupa vašim podacima bežičnim putem. Fizičkom krađom vašeg uređaja napadači bi mogli imati neograničen pristup svim njegovim podacima, kao i svim povezanim računima u oblaku. Poduzimanje mjera za zaštitu vaših uređaja od gubitka ili krađe je važno, ali ako se dogodi najgore, mala priprema može zaštititi podatke u njima. Većina mobilnih uređaja, uključujući prijenosna računala, sada imaju mogućnost potpunog šifriranja svojih pohranjenih podataka—čineći uređaje beskorisnima za napadače koji ne mogu dati odgovarajuću lozinku ili osobni identifikacijski broj (PIN). Uz šifriranje sadržaja uređaja, također je preporučljivo konfigurirati aplikacije vašeg uređaja da zahtijevaju podatke za prijavu prije dopuštanja pristupa bilo kakvim informacijama u oblaku. Na kraju, zasebno šifrirajte ili zaštitite lozinkom datoteke koje sadrže osobne ili osjetljive podatke. To će pružiti još jedan sloj zaštite u slučaju da napadač uspije pristupiti vašem uređaju.

Što možete učiniti da smanjite rizike za svoju bežičnu mrežu?

– Promijenite zadane lozinke. Većina mrežnih uređaja, uključujući bežične pristupne točke, unaprijed je konfigurirana sa zadanim administratorskim lozinkama radi pojednostavljenja postavljanja. Ove zadane lozinke lako su dostupne za dobivanje na mreži i stoga pružaju samo marginalnu zaštitu. Promjena zadanih lozinki napadačima otežava pristup uređaju. Korištenje i povremeno mijenjanje složenih lozinki vaša je prva linija obrane u zaštiti vašeg uređaja. (Pogledajte Odabir i zaštita lozinki.)

– Ograničite pristup. Dopustite samo ovlaštenim korisnicima pristup vašoj mreži. Svaki dio hardvera spojen na mrežu ima adresu kontrole pristupa medijima (MAC). Možete ograničiti pristup svojoj mreži filtriranjem ovih MAC adresa. Konzultirajte svoju korisničku dokumentaciju za određene informacije o omogućavanju ovih značajki. Također možete koristiti “guest” račun, koji je široko korištena značajka na mnogim bežičnim usmjerivačima. Ova vam značajka omogućuje da gostima omogućite bežični pristup na zasebnom bežičnom kanalu s zasebnom lozinkom, a pritom zadržavate privatnost svojih primarnih vjerodajnica.

– Šifrirajte podatke na vašoj mreži. Šifriranje vaših bežičnih podataka onemogućuje svima koji bi mogli pristupiti vašoj mreži da ih vide. Za ovu zaštitu dostupno je nekoliko protokola šifriranja. Wi-Fi zaštićeni pristup (WPA), WPA2 i WPA3 šifriraju informacije koje se prenose između bežičnih usmjerivača i bežičnih uređaja. WPA3 je trenutno najjača enkripcija. WPA i WPA2 su i dalje dostupni;

međutim, preporučljivo je koristiti opremu koja posebno podržava WPA3, jer korištenje drugih protokola može ostaviti vašu mrežu otvorenom za iskorištavanje.

– Zaštitite svoj identifikator skupa usluga (SSID). Kako biste spriječili autsajdere da lako pristupe vašoj mreži, izbjegavajte objavljivanje svog SSID-a. Svi Wi-Fi usmjerivači omogućuju korisnicima zaštitu SSID-a svog uređaja, što napadačima otežava pronalaženje mreže. U najmanju ruku promijenite svoj SSID u nešto jedinstveno. Ostavljanje kao zadano od strane proizvođača moglo bi omogućiti potencijalnom napadaču da identificira vrstu usmjerivača i eventualno iskoristi sve poznate ranjivosti.

– Instalirajte vatrozid. Razmislite o instaliranju vatrozida izravno na svoje bežične uređaje (vatrozid temeljen na hostu), kao i na vašoj kućnoj mreži (vatrozid temeljen na usmjerivaču ili modemu). Napadači koji mogu izravno pristupiti vašoj bežičnoj mreži možda će moći zaobići vaš mrežni vatrozid—vatrozid temeljen na hostu će dodati sloj zaštite podacima na vašem računalu (pogledajte Razumijevanje vatrozida za kućnu i malu uredsku upotrebu).

– Održavajte antivirusni softver. Instalirajte antivirusni softver i ažurirajte definicije virusa. Mnogi antivirusni programi također imaju dodatne značajke koje otkrivaju ili štite od špijunskog i reklamnog softvera (pogledajte Zaštita od zlonamjernog koda i Što je kibernetička sigurnost?).

– Dijeljenje datoteka koristite oprezno. Dijeljenje datoteka između uređaja trebalo bi onemogućiti kada nije potrebno. Uvijek biste trebali odlučiti dopustiti dijeljenje datoteka samo preko kućnih ili poslovnih mreža, nikada na javnim mrežama. Možda biste trebali razmisliti o stvaranju namjenskog direktorija za dijeljenje datoteka i ograničiti pristup svim drugim direktorijima. Osim toga, trebali biste zaštititi lozinkom sve što dijelite. Nikada ne otvarajte cijeli tvrdi disk za dijeljenje datoteka (pogledajte Odabir i zaštita lozinki).

– Održavajte softver vaše pristupne točke zakrpanim i ažuriranim. Proizvođač vaše bežične pristupne točke povremeno će izdavati ažuriranja i zakrpe za softver i firmver uređaja. Obavezno redovito provjeravajte web mjesto proizvođača za ažuriranja ili zakrpe za svoj uređaj.

– Provjerite opcije bežične sigurnosti vašeg internet davatelja ili proizvođača usmjerivača. Vaš pružatelj internetskih usluga i proizvođač usmjerivača mogu pružiti informacije ili resurse koji će vam pomoći u zaštiti vaše bežične mreže. Za konkretne prijedloge ili upute provjerite područje korisničke podrške na njihovim web stranicama.

– Povežite se pomoću virtualne privatne mreže (VPN). Mnoge tvrtke i organizacije imaju VPN. VPN-ovi omogućuju zaposlenicima sigurno povezivanje na svoju mrežu kada su izvan ureda. VPN-ovi šifriraju veze na kraju slanja i primanja i sprječavaju promet koji nije ispravno šifriran. Ako vam je VPN dostupan, svakako se prijavite na njega kad god trebate koristiti javnu bežičnu pristupnu točku.

LITERATURA

https://cuc.carnet.hr/2007/program/radovi/pdf/c-6-rad.pdf

https://www.cert.hr/wp-content/uploads/2019/03/Sigurnost-bezicnih-mreza.pdf

https://pcchip.hr/helpdesk/kako-zastititi-bezicnu-mrezu/

https://security.foi.hr/wiki/index.php/Suvremeni_napadi_na_WI-FI.html

https://www.logsign.com/blog/types-of-wireless-network-attacks/