Sigurnost bežičnih mreža

CERT.hr
surfaj sigurnije

Sadržaj

O Nacionalnom CERT-u

Nacionalni CERT (eng. *Computer Emergency Response Team*) odjel je Hrvatske akademske i istraživačke mreže – CARNET, čija je osnovna zadaća obrada incidenata na internetu odnosno očuvanje informacijske sigurnosti u Republici Hrvatskoj. Nacionalni CERT bavi se incidentom ako se jedna od strana u incidentu nalazi u Republici Hrvatskoj, odnosno, ako je u .hr domeni ili u hrvatskom IP adresnom prostoru, osim tijela državne uprave za koji je nadležan CERT ZSIS (CERT Zavoda za sigurnost informacijskih sustava).

Ovisno o tome kako vam možemo pomoći – za opće informacije nazovite 01 6661 650 ili nam pišite na ncert@cert.hr, a računalno-sigurnosne incidente prijavite na incident@cert.hr. Sve ostale informacije o Nacionalnom CERT-u nalaze se na adresi www.cert.hr.

Uvod

Svijet je danas nezamisliv bez bežičnih mreža. Koriste se za spajanje mobilnih uređaja i računala na internet i praktički omogućuju stalnu povezanost gdje god se nalazili. Čim se povežete na neku bežičnu („WiFi“) mrežu u kafiću, zračnoj luci, negdje na otvorenom ili doma, dobijete trenutačni pristup globalnoj mreži. Trend je da gradovi, odnosno lokalne zajednice i sl., grade svoje bežične mreže kako bi posjetitelji imali pristup internetu. Svim tim mrežama je zajedničko da za komunikaciju putem zraka (radio valovima) koriste protokol **IEEE 802.11.** Međutim, postoje ozbiljni sigurnosni rizici prilikom korištenja takvih mreža. Za krajnje korisnike to znači da spajanjem na nesigurnu mrežu ili mrežu koju kontroliraju zlonamjerni hakeri (*“crackeri”*), mogu odati svoje povjerljive podatke neželjenim osobama. U tom slučaju netko može presresti i špijunirati internetski promet korisnika te tako doći do informacija kao što su lozinke za pristup web servisima i dr.

Također, većina kućanstava posjeduje usmjerivač s bežičnim modulom koji putem radio valova omogućuje spajanje vaših prijenosnih računala, pametnih mobitela, pametnih televizija i ostalih uređaja na internet. Naravno, sve to putem usmjeritelja kojeg kupac dobije od komercijalnog davatelja internet usluge (ISP-a).

Jedna od očitih prednosti bežičnog spajanja je da nije potrebna vezanost kabelom za jedno mjesto. Problem je što se valovi, pomoću kojih se prenose podaci, šire u svim smjerovima te pokrivaju šire područje. Svatko u dometu vaše bežične mreže može se pokušati spojiti na nju i u slučaju da mu to pođe za rukom, može izvršiti razne zlonamjerne radnje. Usmjerivač je potrebno podesiti prema današnjim sigurnosnim standardima kako bi onemogućili zlonamjerne korisnike da koristeći taj pristup internetu ugrožavaju sigurnost ostalih internet korisnika, uključujući onih koji su spojeni na isti uređaj.

Ova brošura daje smjernice korisnicima, ali i vlasnicima uređaja koji omogućuju bežično spajanje na njih, kako ispravno podesiti svoje uređaje kako bi zaštitili sebe, odnosno korisnike koji se spajaju na njihovu bežičnu mrežu (infrastrukturu).

Protokol 802.11

Protokol sam po sebi služi kako bi nešto bilo standardizirano i na identičan način korišteno od strane kako korisnika, tako i proizvođača opreme.

802.11 je grupa protokola donesena od strane IEEE (*Institute of Electrical and Electronics Engineers*), standardizacijskog tijela s ciljem implementacije i razvoja bežične lokalne komunikacije (WLAN). Postoje različite verzije protokola koje se razlikuju po više parametara: brzinama prijenosa, frekvenciji na kojoj rade, udaljenostima na kojima je moguć prijenos podataka te tehnologijama na kojima se zasnivaju. Ono što je najbitnije je da svaka nova verzija donosi veće brzine prijenosa podataka i kompatibilnost s prethodnim standardima. Današnji bežični mrežni uređaji uglavnom koriste **802.11n** i **802.11ac** protokole za prijenos podataka. Prijenos podataka se ovisno o upotrijebljenom protokolu odvija na **2.4 GHz** ili na **5 GHz.** 2.4 Ghz donosi veću pokrivenost signalom, dok 5 Ghz nudi veće brzine prijenosa.

Preporuke za kućne korisnike

Rizici

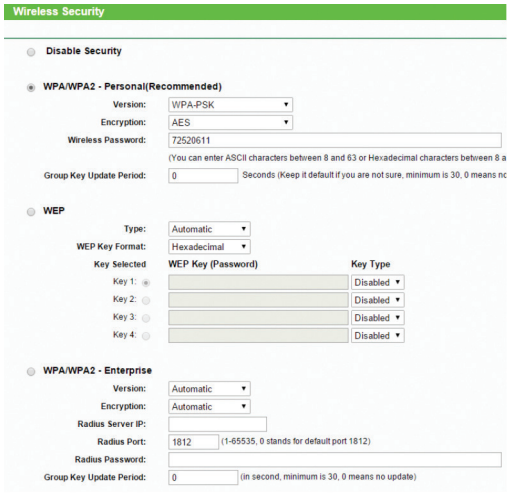
Kad se osoba spoji na mrežu koja je pod vašom administracijom, vi ste odgovorni za sve (potencijalno) nezakonite radnje koje napravi. Popis radnji koje može napraviti je velik, na primjer izvršavanje napada na druge računalne sustave, preuzimanje materijala pod autorskim pravima (intelektualno vlasništvo) ili nekog sadržaja koji upućuje na neku kriminalnu djelatnost. Uz sve to, kad se napadač nalazi u istoj mreži u kojoj ste vi, pomoću različitih programa za prisluškivanje podatkovnog prometa može doznati privatne podatke o vama i vašim navikama na internetu, poput web stranica koje posjećujete i lozinki koje koristite. Također, zlonamjerni korisnik (*„cracker"*) može podići svoju bežičnu mrežu s istim nazivom (**SSID**-om) poput neke legitimne, s namjerom da prisluškuje promet i tako pokuša doći do vrijednih korisničkih podataka, što je još poznato kao *„evil twin"* napad. Posljedica je to činjenice da računala i mobilni uređaji (odnosno njihove bežične kartice), češće odabiru spajanje na mrežu (isti SSID) koja ima jači signal.

Kako podesiti sigurnosne postavke

Jako je bitno pravilno podesiti sigurnosne postavke vaše bežične mreže, odnosno vašeg usmjerivača kako biste spriječili upad „nepozvanih gostiju".

Kad dobijete usmjerivač od vašeg pružatelja internet usluga, prva stvar koja se preporučuje je **promjena inicijalne lozinke** za pristup njegovim postavkama. Svatko tko se nalazi na mreži može se pokušati spojiti na administratorsko sučelje usmjerivača te mijenjati sigurnosne postavke. Na web stranicama pružatelja interneta nalaze se upute za konfiguriranje modela usmjerivača koje isporučuju, a u sklopu kojih se nalaze inicijalne lozinke za pristup njihovoj konfiguraciji.
Jednostavnim isprobavanjem malog broja lozinki moguće je doći do pristupa usmjerivaču u slučaju da vlasnik mreže nije promijenio inicijalnu lozinku.
Druga preporučena stvar je postavljanje **lozinke** i odabir sigurne metode **šifriranja** podataka koji se prenose bežičnim putem. Postavljanjem kratke i jednostavne lozinke poput različitih imena vezanih uz vas ili vašu obitelj, kratkog niza brojeva ili sličnog riskirate da napadač pogodi šifru ili da iskoristi neki od alata koji metodom velikog broja pokušaja i pogreške (*„brute force"*) dolazi do vaše lozinke.

Minimalna preporučena dužina lozinke koju biste trebali postaviti je kombinacija 15 nasumično odabranih brojeva, slova i znakova.



Komunikaciju između računala i usmjerivača je potrebno šifrirati kako napadač ne bi mogao doći do prenesenih podataka. Kad spominjemo bežične mreže, dva najpoznatija i najraširenija protokola su WEP i WPA/WPA2.

WEP (*Wired Equivalent Privacy*) je najstariji protokol za šifriranje bežičnih mreža. Ovaj protokol se sve manje koristi jer je otkriveno više sigurnosnih propusta u samom protokolu zbog kojih je moguće u roku od nekoliko minuta doći do ključa potrebnog za dešifriranje, odnosno spajanje na mrežu. Naslijedio ga je WPA, odnosno WPA2 protokol **(*Wi-Fi Protected Access*)**. Prilikom postavljanja metode šifriranja moguće je odabrati između više različitih verzija WPA protokola: WPA-TKIP (WPA *Personal*), WPA-AES, WPA2-TKIP, WPA2-AES (WPA2 *Personal*), WPA2 *Enterprise*. Preporuka je korištenje WPA2 protokola uz AES metodu šifriranja koja se u slučaju nekih proizvođača naziva **WPA2 *Personal***. Razlika između *Personal* i *Enterprise* verzija je u tome što *Enterprise* verzija koristi dodatni server za autentifikaciju korisnika i pogodna je za poslovne korisnike radi skalabilnosti i lakšeg administriranja. Uz dovoljno dugu lozinku vrlo je teško dešifrirati bežičnu komunikaciju prilikom korištenja WPA2-AES protokola.

U sklopu sigurnog postavljanja usmjerivača bitno je spomenuti **WPS (*WIFI Protected Setup*)** opciju, koja je osmišljena za jednostavnije spajanje bežičnih uređaja bez dodatnih konfiguracija i znanja lozinke. Postoji više implementacija samog rješenja. Prva implementacija je u obliku PIN-a koji se sastoji od 8 znamenki i obično se nalazi na poleđini usmjerivača. Dovoljno je pročitati taj PIN i upisati ga u prijenosni uređaj koji želite spojiti na mrežu. Nakon upisanog PIN-a usmjerivač automatski šalje uređaju sve postavke (uključujući i lozinku za šifriranje podataka) kako bi se mogao spojiti na bežičnu mrežu. Metodom pokušaja pogađanja PIN-a moguće je u kraćem vremenskom intervalu doći do lozinke. Druga implementacija uključuje WPS tipku (fizički na usmjerivaču ili softverski u postavkama usmjerivača).

Pritiskom tipke omogućuje se spajanje korisničkog uređaja na bežičnu mrežu bez upisivanja lozinki ili PIN-ova.
WPS opcija predstavlja veliki sigurnosni problem (posebno verzija s upisivanjem PIN-a jer ne zahtijeva fizički pristup usmjerivaču). Preporuka je njezino onemogućavanje.

Mitovi o postavkama sigurnosti

U nastavku slijede opisi nekih glavnih mitova koji su popularni kod korisnika i pružatelja bežičnih mreža.

- **WEP metoda šifriranja** je dovoljna metoda zaštite - slažemo se da je ikakva zaštita bolja nego nikakva, ali WEP šifriranje nije dovoljno sigurno za korištenje.
- **Ograničavanje oglašavanja (skrivanje SSID-a)** - svaka bežična mreža posjeduje neki identifikator prema kojem je prepoznatljiva, odnosno SSID. Ako se isključi oglašavanje bežične mreže, ona se neće pojaviti u popisu dostupnih mreža na vašem računalu ili mobitelu, ali korištenjem odgovarajućeg alata napadač može lako doći do SSID-a.
- **Filtriranje po MAC adresama** – svako računalo na svijetu bi trebalo imati jedinstvenu hardversku adresu – MAC adresu. Usmjerivači imaju ugrađenu funkciju da se omogući spajanje računalima sa samo određenim MAC adresama i tako možete zaštititi svoju mrežu od drugih. Danas postoje alati koji po potrebi mijenjaju vašu MAC adresu. Napadaču je dovoljno postaviti MAC adresu svog računala da bude identična računalu koje ima dopuštenje za spajanje na mrežu.
- **Limitiranje ili isključivanje DHCP poslužitelja** – da bi računalo moglo pristupiti internetu, potrebno mu je dodijeliti lokalnu IP adresu kako bi mogao komunicirati s usmjerivačem. Taj posao dodjele obično obavlja usmjerivač, i u slučaju da isključimo tu funkciju (dodjela IP adresa putem DHCP poslužitelja) teoretski bismo onemogućili napadača. Napadač samo treba doznati adresu mreže i statički konfigurirati IP adresu iz tog raspona da bi omogućio daljnju komunikaciju s usmjerivačem, odnosno izlaz na internet.
- **Limitiranje jačine signala** – i u slučaju da smanjite jačinu signala na najmanju vrijednost i tako ograničite pokrivanje signalom na jednu prostoriju u vašem domaćinstvu, na tržištu postoje mrežne kartice sa snažnim antenama koje hvataju signal i na udaljenostima većim od kilometar.

Redovite nadogradnje firmwarea

Kao što redovito instalirate najnovije zakrpe za svoj operacijski sustav kako biste poboljšali sigurnost vašeg računala, tako je i jako bitno instalirati nove verzije ***firmwarea*** **(ugradbenog softvera)** na vaš usmjerivač sukladno njihovim objavljivanjima.
Kad usmjerivač krene u prodaju (odnosno masovno korištenje) korisnici otkrivaju dotad nepoznate probleme koji se rješavaju izdavanjem zakrpa. Ako je verzija vašeg firmwarea zastarjela, napadač može iskoristit poznatu ranjivost kako bi pristupio vašoj mreži, odnosno računalima koja se nalaze u njoj.

Za korisnike otvorenih mreža

Jako je veliki broj osoba koje koriste internet na dnevnoj bazi za razne akcije i pri tom ne biraju način kako doći do pristupa. Sve se više koriste otvorene mreže za tu namjenu. Problem kod otvorenih mreža je taj da one postaju popularnije i zlonamjernim hakerima koji ih koriste za zlonamjerne radnje poput krađe podataka. Takvi korisnici se mogu pozicionirati između vas i pristupne točke te tako dobiti pristup osjetljivim podacima o vama (važnim mailovima, informacijama o kreditnoj kartici, pristupnim podatcima za spajanje na web portale...).

U nastavku su opisane radnje kojima je moguće poboljšati vašu sigurnost prilikom korištenja otvorenih mreža:

- **Korištenje VPN-a (*Virtual Private Network*)** – VPN radi na principu da šifrira sav internetski promet između korisnika i web servera pružatelja VPN usluge. Pružatelj usluge je posrednik koji prosljeđuje promet na odredišne lokacije i vraća šifrirane odgovore korisniku. Mnogi proizvođači antivirusnog softvera nude dodatnu opciju kupnje VPN-a. Dok korisnik koristi VPN, sve što zlonamjerni haker može napraviti je pozicionirati se između korisnika i njegove pristupne točke i dobiti uvid u šifrirani promet koji je za njega nečitljiv.
- **Korištenje SSL (*Secure Sockets Layer*) konekcija** – SSL je protokol namijenjen sigurnom prijenosu privatnih podataka na internetu. Poput VPN-a koristi šifriranje za prijenos istih. Web stranica koja koristi SSL protokol za šifriranje podataka između nje i vašeg preglednika započinje s „https:“ umjesto s „http:“.
- **Isključivanje dijeljenja podataka** – jedna od stvari koju sigurno ne želite učiniti prilikom spajanja na nesigurnu otvorenu mrežu je dijeljenje datoteka s ostalim korisnicima mreže.
- **Isključivanje bežične kartice kad se ne koristi** – u uvodu je spomenuto da se mrežna kartica spaja na pristupnu točku koja emitira jači signal. Osim toga, bežična kartica se automatski spaja na mrežu na koju je nekad u prošlosti bila spojena (prema SSID-u). Podizanjem vlastite bežične mreže identične onoj na kojoj je uređaj bio spojen haker inicira spajanje bežične kartice (uređaja) na nju.

Za vlasnike otvorenih bežičnih mreža

Kao i u slučaju kućnih bežičnih mreža, tako i kod otvorenih bežičnih mreža postoje određeni rizici za vlasnike. Vlasnik otvorene mreže je i dalje jedina kontakt i odgovorna osoba za sve potencijalno nezakonite radnje koje se odvijaju u njegovoj mreži. To kao posljedicu uvodi nužnost uvođenja autentifikacije krajnjih korisnika prije nego li im se dopusti korištenje mreže. Pohranjivanjem određenih podataka o korisnicima, poput podataka o uređajima pomoću kojih se spajaju, podataka o nečemu što ih identificira (broj mobilnog uređaja/mail adresa...) te pohranjivanje vremena njihovih spajanja na mrežu, uvodi se mogućnost praćenja korisnika i prebacivanje odgovornosti za zlonamjerna djela koje oni naprave koristeći vašu mrežu.

Uvjeti korištenja

Prije dopuštanja korištenja bežične mreže preporučuje se upozoriti korisnika na prihvatljivo korištenje iste. Korisnici javnih otvorenih bežičnih mreža, ali i onih privatnih na mjestima poput hotela, restorana i zračnih luka, moraju biti točno upoznati s pravilima i rizicima korištenja takve mreže.

Najčešće je dovoljno implementirati rješenje čija je uloga preusmjeravanje korisnika na početnu web stranicu na kojoj su napisani uvjeti korištenja.

Korisnike je potrebno upoznati s:

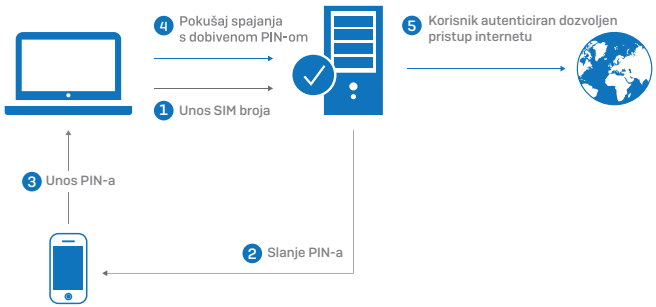
- vrstom usluge (osnovni tehnički parametri),
- mogućnosti blokiranja pristupa u slučaju kršenja pravila,
- nezajamčenom sigurnosti, odnosno privatnosti korištenja mreže
- ograničavanjem od odgovornosti vlasnika (operatora) mreže za potencijalnu štetu koju je korisnik pretrpio,
- zabranom korištenja mreže za zlonamjerne radnje (širenje spama, DDoS, kršenje autorskih prava...).

Rješenja za autentifikaciju korisnika

SMS

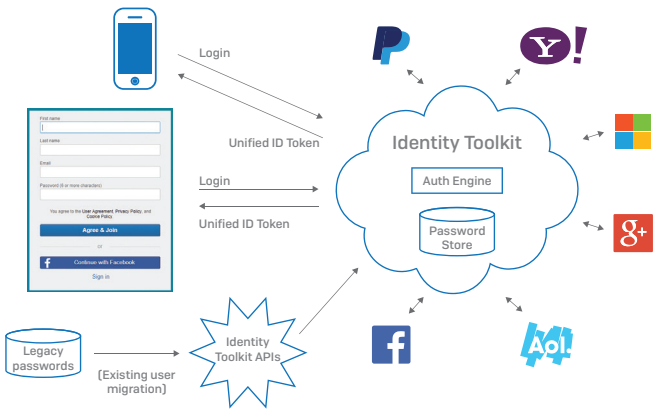
Jednostavna implementacija uključuje autentifikaciju korisnika na temelju nečeg što on posjeduje. Svaki korisnik posjeduje mobilni uređaj sa SIM karticom, stoga je ovo adekvatno rješenje.

U slučaju SIM kartice korisnik prilikom pokušaja korištenja interneta unosi broj svog mobilnog telefona na kojeg se potom šalje SMS poruka s PIN-om određene dužine. Korisnik potom unosi PIN u web sučelje i s tim dokazuje da telefonski broj pripada njemu. Na strani pružatelja usluge nalazi se jednostavan server/baza podataka koja uparuje PIN s telefonskim brojem na koji je poslan. Kod prvog upisivanja PIN-a u web obrazac pamti se MAC adresa uređaja s kojeg se spaja i uparuje se s PIN-om kojeg unosi.
Prilikom ponovnog pokušaja spajanja korisnika provjerava se postoji li asocijacija PIN-a i MAC adrese uređaja s kojeg se korisnik pokušava spojiti i u slučaju da postoji, dopušta se korištenje interneta, u suprotnom se prikazuje početna stranica za autentifikaciju putem SIM kartice (mobilnog uređaja).
Naprednija izvedba ovog rješenja uključuje bilježenje aktivnosti svakog korisnika i spremanje tih aktivnosti u bazu podataka radi kasnije eventualno potrebne forenzike.



Primjer – agregacija autentifikacija

Zanimljivo rješenje za autentifikaciju korisnika dolazi od strane Googla u obliku Google *Identity Toolkit*-a. Ono u sebi sadrži višestruke opcije autentifikacije korisnika. Korisnik se može autenticirati pomoću različitih servisa: Google, Facebook, Yahoo, Microsoft, PayPal i dr. Njegova prednost je u tome što u sebi objedinjuje velike servise koje koristi veliki broj ljudi te na jednom mjestu rješava problem autentifikacije korisnika. Korištenje ovog rješenja je zahtjevnije za implementaciju jer je potrebno uvođenje posredničkog servera na kojem bi se održavale informacije o autentificiranim klijentima i njihovim pristupnim podatcima.



Radius

Radius server je rješenje za autentifikaciju korisnika pogodan za velika poslovna okruženja u kojima se nalazi veliki broj korisnika. Njegova prednost je što na centralnom mjestu sprema informacije o korisnicima i istovremeno omogućuje laku administraciju istih. Podaci o korisnicima mogu biti spremljeni u sklopu samog RADIUS servera ili pak u već postojećoj bazi podataka (npr. LDAP). Veliki broj organizacija već posjeduje postojeću bazu korisnika, stoga je ovo drugo rješenje učestalije. RADIUS server u tom slučaju služi kao posrednik koji prima zahtjeve klijenta i omogućuje/ograničava njihov pristup resursima.

Primjer - autentifikacija u hotelima

Jedna od mogućih opcija za autentifikaciju gosta u hotelu je povezivanje prezimena gosta i broja sobe u kojoj odsjeda. Prilikom prijavljivanja gosta na recepciji hotela podaci o klijentu se šalju u središnju bazu podataka u kojoj se nalaze podaci o svim gostima i pripadajući brojevi soba u kojima odsjedaju. Sav internetski promet koji dolazi od neautentificiranog uređaja se presreće te preusmjerava na tzv. *"captive portal"* u kojem gost mora unijeti tražene podatke. U slučaju da se podaci podudaraju s onima spremljenim u bazi, gostu se omogućuje pristup internetu. Prilikom odjavljivanja gosta na recepciji hotela, iz sustava se briše asocijacija prezime gosta-broj sobe i tako se održava ažurnost.

Hrvatska akademska
i istraživačka mreža – CARNET
Josipa Marohnića 5, 10000 Zagreb, Hrvatska
tel: +385 1 6661 616, mail: ured@carnet.hr

CERT.hr
surfaj sigurnije
tel: +385 1 6661 650, mail: ncert@cert.hr,
www.cert.hr

11/2018.