SANS SECURITY AWARENESS

Vaš mesečni bilten za podizanje svesti o bezbednosti informacija

Virtuelne privatne mreže (VPN)

Uvod

Neretko vam je potrebno da koristite javni Wi-Fi za pristup internetu kada niste kod kuće (npr. kad ste u lokalnom restoranu ili kafiću) ili kada putujete (u hotelu ili na aerodromu). Koliko su zapravo bezbedne ove mreže i ko sve gleda ili snima vaše aktivnosti na internetu? Možda ne verujete ni vašem provajderu kućnog interneta (ISP) i želite da budete sigurni da ne može da prati šta radite na internetu. Zaštitite vaše aktivnosti na internetu i sačuvajte vašu privatnost korišćenjem VPN-a, virtuelne privatne mreže (eng. Virtual Private Network). VPN je tehnologija koja kreira privatni, šifrovani tunel za vaše aktivnosti na internetu, što u mnogome otežava praćenje ili nadgledanje onoga što na internetu radite. Pored toga, VPN vam pomaže i da sakrijete vašu lokaciju i na taj način otežava sajtovima koje posećujete da odrede gde se nalazite.

Kako radi VPN?

VPN funkcioniše tako što kreira privatni, šifrovani tunel do pružaoca VPN usluge koga odaberete. Sve vaše aktivnosti na mreži prolaziće kroz ovaj tunel, a zatim će iz mreže vašeg VPN provajdera dospevati na željeno odredište. Na primer, ako se nalazite u Kragujevcu i povežete se sa VPN serverom u Minhenu u Nemačkoj, svaki veb sajt koji posetite će verovati da se povezujete iz Minhena. VPN je jednostavan za korišćenje. Prvi korak je pronalaženje VPN provajdera kome verujete i kreiranje naloga kod tog provajdera (ovo obično zahteva kupovinu njihove usluge). Nakon kreiranja naloga moći ćete da preuzmete, instalirate i konfigurišete VPN softver. Kada jednom instalirate i konfigurišete softver, povezujete se na Internet kao i obično. VPN softver u pozadini kreira vaš šifrovani tunel i štiti vašu privatnost, a da vi toga čak niste ni svesni.

Izbor VPN provajdera

Vaša privatnost i vaše aktivnosti na internetu bezbedne su samo onoliko koliko je to vaš VPN provajder. Postarajte se da izaberete provajdera od poverenja. U nastavku teksta navedene su ključne stavke za izbor VPN provajdera.

Beleženje logova: Potražite servis koji ne čuva nikakve logove i kome je fokus na privatnosti. Ako vaš provajder VPN servisa ne prikuplja nikakve logove, onome ko pokuša da se vrati unazad i vidi šta ste radili na internetu biće mnogo teže da to učini.

Gde je sedište kompanije: Različiti VPN provajderi su locirani u različitim zemljama. Postarajte se da izaberete VPN provajdera koji ima sedište u zemlji sa strogim zakonima u oblasti zaštite privatnosti. Provajderi VPN-a koji se nalaze u zemljama koje imaju nedovoljnu ili slabu regulativu u oblasti zaštite privatnosti mogu biti primorani da otkriju informacije koje prikupljaju o vama.

Serveri: Potražite VPN uslugu koja ima servere koji se nalaze u zemljama ili gradovima koji su vam potrebni. Neki VPN provajderi imaju hiljade servera i lokacija širom sveta. Ako imate potrebu da vaše konekcije ka internetu izgledaju kao da dolaze iz neke određene zemlje, proverite da li VPN provajder može to da vam pruži?

Kompatibilnost: Potražite servise koji rade na različitim računarima i mobilnim uređajima. Na primer, pretpostavimo da koristite laptop sa MS Windows operativnim sistemom, tablet i iPhone. Biće vam potrebna VPN usluga koja će raditi na svim tim uređajima.

Izbegavajte besplatne usluge: Budite veoma oprezni kada su u pitanju "besplatne" VPN usluge i uvek se zapitajte kako zarađuju i opstaju? Besplatni servisi mogu prikupljati i prodavati vaše informacije.

VPN je odličan način da zaštitite vašu privatnost na internetu. Međutim, VPN ne čini ništa da zaštiti vaš računar, uređaje ili vaše onlajn naloge. Čak i ako koristite VPN, postarajte se da se uvek pridržavate osnovnih bezbednosnih preporuka, redovno ažurirajte vaše uređaje, koristite zaključavanje ekrana i uvek upotrebljavajte jake, jedinstvene lozinke za sve vaše naloge.

Verzija na srpskom

Telekom Srbija kao društveno odgovorna telekomunikaciona kompanija pomaže prevođenje i distribuciju ovog biltena kako bi se unapredila svest korisnika informaciono-komunikacionih tehnologija o bezbednosti informacija.

Gost urednik

Fil Džonsi *(@peakreflections) je IT stručnjak iz Palm Biča sa iskustvom iz bezbednosti, forenzike i revizije Fil poseduje SANS sertifikate iz digitalne forenzike, osnova bezbednosti i jedan je od recenzenata u OUCH zajednici. Njegova strast je da IT bezbednost učini jednostavnom za druge.*

Dodatni materijal

Napravite lozinku na jednostavan način:	https://www.sans.org/u/Sd8
Kako da zaštitite vaše mobilne uređaje:	https://www.sans.org/u/Sdd
Zaštitite se od malvera:	https://www.sans.org/u/Sdi