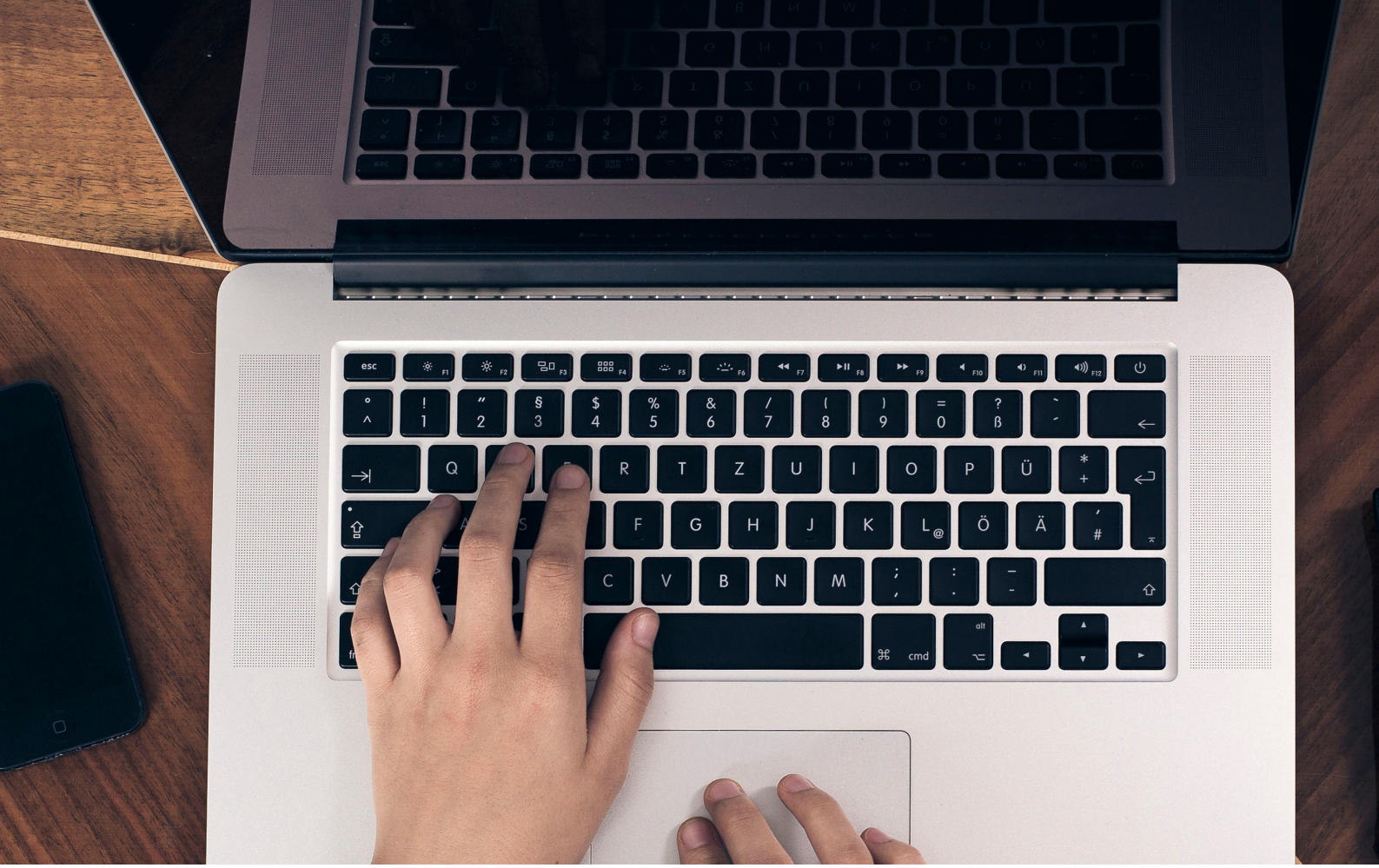

VPN ZA MALA I SREDNJA PREDUZEĆA

PRIJAVITE SVAKI INCIDENT
NA NAŠEM PORTALU

SRB-CERT

VPN

U današnje vreme, u pogledu bezbednosti, kako u privatnom tako i u poslovnom okruženju, od najveće važnosti je zaštita podataka i informacija koje razmenjujemo svakodnevno putem interneta.

Ukoliko se korisnici nalaze van kuće, u nekom restoranu, hotelu, aerodromu ili drugom javnom mestu, najveći broj njih će koristiti bežične javne tačke za pristup internetu, odnosno WiFi. Posmatrano sa bezbednosnog aspekta, najveći izazov predstavlja sigurnost korišćenja ovakvih pristupnih tačaka, jer korisnici nemaju uvid ko sve koristi navedenu tačku za pristup i da li se nadgleda i snima razmena podataka putem te WiFi pristupne tačke.

Kada govorimo o potrebi korisnika za radom na daljinu, odnosno radom od kuće, koji podrazumeva pristupanje resursima software-as-a-service (SaaS), koji pripadaju određenoj organizaciji ili instituciji, neophodno je da se takav rad obavlja na bezbedan način, kako ne bi došlo do moguće kompromitacije podataka kojima korisnik pristupa.

Kako bi korisnici zaštitili svoje mrežne aktivnosti, privatnost i sprečili da dođe do kompromitacije podataka organizacije preporuka je korišćenje virtuelne privatne mreže, odnosno VPN (eng. Virtual Private Network) pristup. VPN tehnologija kreira privatni, šifrovani tunel za aktivnosti na mreži i znatno otežava bilo kome da prati ili nadgleda šta korisnik radi dok je na mreži. Takođe, VPN tehnologija omogućava kompanijama bolju zaštitu od mogućeg gubitka i kompromitacije podataka, tako što se između korisničke mreže, bilo da se koristi javni ili privatni WiFi, pravi bezbedan i šifrovan tunel, preko javnog interneta do mreže organizacije.

ŠTA JE VPN I KAKO RADI?

VPN je jednostavan način povezivanja različitih mreža koje su odvojene od Interneta, koristeći sigurnosne protokole koji omogućavaju autentičnost i poverljivost informacija koje putuju VPN vezom ili mrežnim sistemom.

Aplikacije koje se obično koriste, bilo da su imejl, veb, poruke, društvene mreže i sl, zasnivaju se na IP (Internet Protocol) protokolu. Iako su razvijeni određeni standardi, nisu sve internet aplikacije bezbedne, određen broj aplikacija i dalje nije usaglašen sa važećim propisima o načinu deljenja i zaštite podataka. Neujednačen stav o načinu zaštite podataka ostavlja prostora mogućim zloupotrebama od strane napadača, odnosno hakera, koji zbog ovakvih propusta jednostavno mogu doći do ličnih podataka korisnika, kao što su broj tekućeg računa, kreditne kartice, kućne adrese i sl.

VPN kreira privatni tunel preko otvorenog interneta. Ideja je da sve što korisnik pošalje bude enkapsulirano i šifrirano u ovom privatnom komunikacijskom kanalu, pa čak i ako dođe do presretanja poslatih paketa, isti ne mogu biti dešifrovani. VPN predstavlja vrlo moćan i važan alat u zaštiti i bezbednosti korisnika i njihovih podataka, ali ima i svoja ograničenja. Ovde se postavlja pitanje ograničenja VPN-a i razumevanje gde se nalazi krajnja tačka VPN servera. Ukoliko se korisnik nalazi u Srbiji, a povezuje se na VPN server u drugoj državi, celokupan saobraćaj na internetu će biti prikazan kao da je korisnik pristupio iz mreže te druge države, odnosno neće biti vidljivo da je korisnik pristupio iz IP opsega Republike Srbije.

TIPOVI VPN-A

Dva najčešće tipa VPN-a su: korporativni ili poslovni VPN servis koji predstavlja poslovno orijentisano rešenje koje omogućava zaposlenima da se udaljeno povežu na korporativnu mrežu i korisnički VPN servis koji pojedincima omogućava

Većina kompanija ima svoje filijale ili jedinice koje su geografski udaljene, a povezivanje takvih lokacija iznajmljenim privatnim linijama može biti skupo, pa ih povezuju putem javnog interneta, kriptujući podatke tako što koriste korporativni ili poslovni VPN. Korporativni ili poslovni VPN karakteriše ista organizacija koja kontroliše obe krajnje tačke VPN-a. Ako kompanija kontroliše početnu tačku (recimo prodajnu filijalu) i krajnju tačku (poput VPN servera u vašem korporativnom sedištu), možete biti prilično sigurni da se korisnički podaci sigurno prenose.

Korisnički VPN koriste oni koji često borave na javnim mestima, poput hotela, restorana, aerodroma i sl, a povezuju se na veb aplikacije poput društvenih mreža, imejla, banaka ili veb stranica za online kupovinu. Korisnički VPN servis predstavlja dodatni vid zaštite takve komunikacije.

Korisnički VPN servis se u osnovi nudi softver kao usluga (software-as-a-service - SaaS). VPN servis pruža siguran tunel između računarskog uređaja (bilo laptopa, telefona ili tableta) i njihovog servisa data centra. Važno je razumeti da korisnički VPN servis štite prenos podataka sa lokacije korisnika na njihovu lokaciju, a ne od lokacije korisnika do odredišne aplikacije kojoj korisnik želi da pristupi.

Ovde su bitne dve stavke: Prva, ukoliko korisnik pristupa internetu koristeći https protokol, te podatke šifruje pretraživač, a zatim i VPN aplikacija. U VPN data centru podaci korisnika se dešifruju samo jednom, a originalna enkripcija koju nudi pretraživač ostaje neizmenjena. Tako šifrovani podaci se zatim prenose na odredišnu aplikaciju, poput banke korisnika. Druga veoma bitna stavka je da veb aplikacija sa kojom korisnik komunicira ne vidi korisničku IP adresu. Umesto toga, ona će videti IP adresu koja je u vlasništvu VPN servisa, a to korisniku omogućava određeni nivo anonimnog umrežavanja.

INSTALACIJA VPN-A

Što se tiče poslovnog okruženja, preporuka je korišćenje onih alata koji se nalaze u tehničkom okviru i odobreni su od strane poslodavca.

Upravo iz tog razloga, poslodavac najčešće ima unapred definisane tehničke alate koji zaposlenima omogućavaju neometan i bezbedan rad sa udaljenih lokacija, prilikom korišćenja službenih laptopova ili mobilnih uređaja. Ovde se prioritetno misli na korišćenje firewall-a i antivirusne zaštite, zajedno sa bezbednosnim funkcijama kao što su VPN i dvofaktorska autentifikacija. Zašto je to važno: Alati poslodavca koji služe za bezbednost dizajnirani su tako da zaštite podatke i uređaje. Zlonamerni korisnici (hakeri) imaju interes da prikupe sve raspoložive tipove podataka, bilo da radite u kancelariji ili od kuće. U poslovnom okruženju, IT administrator najčešće instalira i podešava VPN, i kreira odgovarajuće uputstvo za korišćenje VPN-a u skladu sa procedurama i politikama poslodavca.

Kada se radi o fizičkim licima korisnički VPN servis je veoma jednostavan za upotrebu. Prvi korak je pronalaženje odgovarajućeg VPN provajdera, a zatim kreiranje naloga (obično podrazumeva kupovinu njihove usluge). Nakon kreiranja korisničkog naloga, neophodno je preuzimanje, instaliranje i konfigurisanje VPN softvera, a zatim se korisnik povezuje na internet. Pokretanjem VPN softvera, korisnik kreira šifrovani tunel za razmenu podataka, koji pruža odgovarajuću zaštitu.

Mrežne aktivnosti korisnika su sigurne i ostaju privatne samo ukoliko to obezbedi izabrani VPN provajder. Preporuka korisnicima je da odaberu odgovarajućeg VPN provajdera u skladu sa svojim potrebama. Neke od ključnih tačaka prilikom odabira odgovarajućeg pružaoca VPN usluga mogu biti:

- **Logovanje:** Odaberite uslugu koja ne čuva logove i fokusirana je na privatnost. Ukoliko pružalac VPN usluge ne sakuplja nikakve logove, mnogo je teže da neko pretraži i uvidi šta je korisnik radio dok je bio na mreži.
- **Gde je osnovana kompanija:** Različiti VPN provajderi pružaju svoje usluge korisnicima širom sveta. Preporuka je da korisnici izaberu VPN provajdera sa sedištem u onim državama koje imaju dobro razvijene zakone o zaštiti podataka. VPN provajderi smešteni u zemljama koje imaju slabe zakone o privatnosti mogu biti primorani da daju informacije koje prikupe o korisnicima.
- **Serveri:** Odaberite VPN uslugu koja ima servere u zemljama ili gradovima koji odgovaraju vašim potrebama. Neki VPN provajderi imaju veliki broj servera i lokacija širom sveta. Sve naravno zavisi od potreba korisnika, a tu se postavlja pitanje: Da li korisnik ima potrebu da veze koje uspostavlja izgledaju kao da dolaze iz određene zemlje? Da li VPN provajder može to da pruži?
- **Kompatibilnost:** Pronađite pružaoce usluge koji rade na različitim operativnim sistemima i mobilnim uređajima. Na primer, korisnik može imati Windows operativni sistem na laptopu, Android tablet i iPhone mobilni telefon, i potrebu da VPN usluga radi na svim tim uređajima.
- **Izbegavajte besplatne usluge:** Budite veoma oprezni prema „besplatnim“ VPN uslugama. Postavlja se pitanje na koji način takvi VPN provajderi zarađuju novac i ostaju u poslu? Pružaoci besplatnih usluga mogu prikupljati i prodavati podatke korisnika, tako da je važno obratiti pažnju na uslove koje nude.

KADA JE POTREBNO KORISTITI VPN?

Kada se radi o poslovnom okruženju, već je napomenuto da svaki put kada su geografski udaljene lokacije (bilo da je u pitanju rad od kuće ili druga filijala) koje treba da se povežu preko javnog interneta, treba razmisliti o korišćenju VPN tehnologije, koja korisniku može pomoći da zaštiti razmenu podataka tokom rada od kuće ilisa druge lokacije.

VPN pruža sigurnu vezu između zaposlenih i poslodavca šifrovanjem podataka i skeniranjem uređaja na zlonamerni softver poput virusa, ransomvera i sl. U tom slučaju će VPN softver verovatno biti pokrenut na ruteru, serveru ili namenskom hardverskom uređaju za VPN server.

Veoma je važno da korisnik uključi VPN kada radi od kuće ili sa druge udaljene lokacije i pristupa podacima ili razmenjuje bitne poslovne informacije. VPN omogućava zaštitu od zlonamernih korisnika (hakera) i onemogućava im da vide šta korisnik radi na mreži tokom radnog dana, što uključuje slanje ili primanje finansijskih informacija, strateških dokumenata i podataka o klijentima. VPN pomaže da se te informacije sačuvaju od zlonamernih korisnika (hakera), ali i konkurenata.

Kada se korisnik koji radi van kuće ili kancelarije, povezuje se na internet, najčešće putem WiFi mreže koja je u vlasništvu hotela, restorana, aerodroma ili druge javne ustanove. U ovim situacijama, korisnik nema saznanja ko još koristi istu pristupnu tačku bežičnom internetu i samim tim može doći do zloupotrebe putem presretanja saobraćaja na mreži. Preporuka Nacionalnog CERT-a je da korisnik uvek kada je van kancelarije ili kuće, a koristi tuđu WiFi mrežu (čak i člana porodice ili prijatelja, jer nemate saznanje da li su bili ugroženi), koristi VPN. Posebno je važno ukoliko korisnik pristupa uslugama koje zahtevaju lične podatke. Imajte na umu da se mnogo toga događa iza scene što nije vidljivo, a nikad se zapravo ne zna da li jedna ili više korisničkih aplikacija potvrđuju autentičnost u pozadini i dovode podatke u rizik.

PREDNOSTI I NEDOSTACI VPN-A

PREDNOSTI

Poboljšava bezbednost. Kada se korisnik poveže na mrežu putem VPN-a, podaci se prenose putem bezbednog i šifrovanog tunela. Na ovaj način su informacije zaštićene od svakog ko pokušava da pristupi ličnim podacima i drugim podacima koje tom prilikom korisnik razmenjuje.

Udaljeni pristup. U slučaju kompanija, velika prednost posedovanja VPN-a je ta što se informacijama može pristupiti udaljeno, od kuće ili sa bilo kog drugog mesta. Na ovaj način VPN može povećati produktivnost kompanije.

Anonimnost na mreži. Kroz VPN korisnik može surfovati internetom potpuno anonimno. U poređenju sa skrivanjem IP adresa putem softvera ili veb proksija, prednost VPN usluge je ta što korisniku omogućava pristup veb aplikacijama i veb stranicama potpuno anonimno. Privatnost se štiti tako što se maskiraju informacije poput IP adrese, lokacije i istorije pretrage, kako ih ne bi pratili veb sajtovi, internet pretraživači i drugi.

Bolje performanse. Širina propusnog opsega i efikasnost mreže se obično mogu povećati nakon primene VPN rešenja.

Smanjuje troškove. Jednom kada se kreira VPN mreža, troškovi održavanja su vrlo niski. Štaviše, ako korisnik odabere provajdera servisa, podešavanje mreže i nadzor nisu više briga korisnika.

PREDNOSTI I NEDOSTACI VPN-A

NEDOSTACI

Najbolji VPN-ovi, nisu besplatni. Pružaoci besplatnih usluga mogu prikupljati i prodavati vaše podatke, jer se postavlja pitanje na koji način zarađuju. Većina njih ne koristi šifrovanje ili nisu pravilno konfigurisani, a na taj način privatnost korisnika na internetu je ugrožena i postoji mogućnost da zlonamerni korisnici presretnu saobraćaj i dođu u posed korisničkih podataka. Takođe, neki besplatni VPN-ovi mogu da korisnika izlože zlonamernom softveru, prodaju propusni opseg botnetima ili čak prikupljaju lične podatke i prodaju ih oglašivačima ili trećim stranama. Na kraju, ukoliko korisnik želi da podaci budu sigurni, neophodno je platiti pouzdanu VPN uslugu.

VPN-ovi izvorno ne rade na svim platformama. VPN-ovi obično rade na najpopularnijim uređajima i operativnim sistemima, ali još uvek postoje neke platforme koje nemaju njihovu podršku, kao što su neki tipovi pametnih televizora, konzole za igranje (Xbox, PlayStation) i sl. U tom slučaju neophodno je da korisnik postavi VPN vezu na ruter, što može biti prilično složen proces i na taj način svaki uređaj pristupaće internetu putem tog rutera koristeći VPN koji je kreiran. Alternativno, VPN vezu korisnik može deliti i putem računara ili laptopa povezivanjem uređaja sa eternet kablom. Međutim, ovakvim povezivanjem korisnik može usporiti performanse mreže ili smanjiti protok, a dodatni izazov predstavlja povezivanje većeg broja uređaja putem računara ili laptopa.

Korišćenje VPN-a može smanjiti brzinu veze. Jedan od glavnih nedostataka VPN usluge sa kojim korisnici imaju problem jeste smanjena brzina veze. Iako se to ne događa svaki put kada korisnik koristi VPN za pristup internetu, brzina mreže se nekad može usporiti, a to se obično dešava u sledećim slučajevima: kada je šifrovanje prejako, VPN protokol koji korisnik upotrebljava nije optimizovan za brzinu i zato što je udaljenost između VPN servera koji korisnik koristi i korisničkog uređaja prevelika. Naravno, postoje i drugi faktori koji mogu uticati, ali to su najčešći razlozi zbog kojih se brzina veze može malo usporiti kada koristite VPN.

Neki VPN-ovi sakupljaju korisničke podatke. Neki provajderi VPN usluga sakupljaju korisničke podatke, najčešće su to informacije o njihovoj konekciji, ali ponekad mogu sakupljati i čuvati lične podatke. Većina provajdera to radi kako bi se pridržavali zakona svojih zemalja. Iako je to razumljivo, VPN koji sakuplja i čuva korisničke podatke, prilično utiče na osnovnu ideju upotrebe VPN-a, a to je integritet podataka. Ovaj problem se može izbeći ukoliko se odabere VPN provajder koji ima strogu i jasnu politiku koja ne sakuplja i ne čuva podatke ili provajdera sa sedištem u zemlji koja ima jake zakone o privatnosti.

ZAKLJUČAK

VPN je najbolji način da se zaštiti privatnost korisnika na mreži.

Međutim, VPN ne radi ništa na obezbeđivanju računara, uređaja ili mrežnih naloga. Čak i ako korisnik upotrebljava VPN, bitno je da uvek sledi osnovne mere zaštite, uključujući redovno ažuriranje uređaja, zaključavanje ekrana i korišćenje jakih, jedinstvenih lozinki za sve korisničke naloge.

Nacionalni CERT Republike Srbije ne promoviše ili favorizuje bilo koji od korišćenih javnih izvora, među kojima su i komercijalni proizvodi i usluge. Sve preporuke, analize i predlozi dati su u cilju prevencije i zaštite od bezbednosnih rizika.

Izvori:

https://www.sans.org/security-awareness-training/resources/virtual-private-networks-vpns

https://uk.norton.com/internetsecurity-how-to-your-essential-4-step-guide-to-using-a-vpn-to-secure-your-network.html

https://us.norton.com/internetsecurity-privacy-benefits-of-vpn.html

https://www.zdnet.com/article/vpn-services-the-ultimate-guide-to-protecting-your-data-on-the-internet/