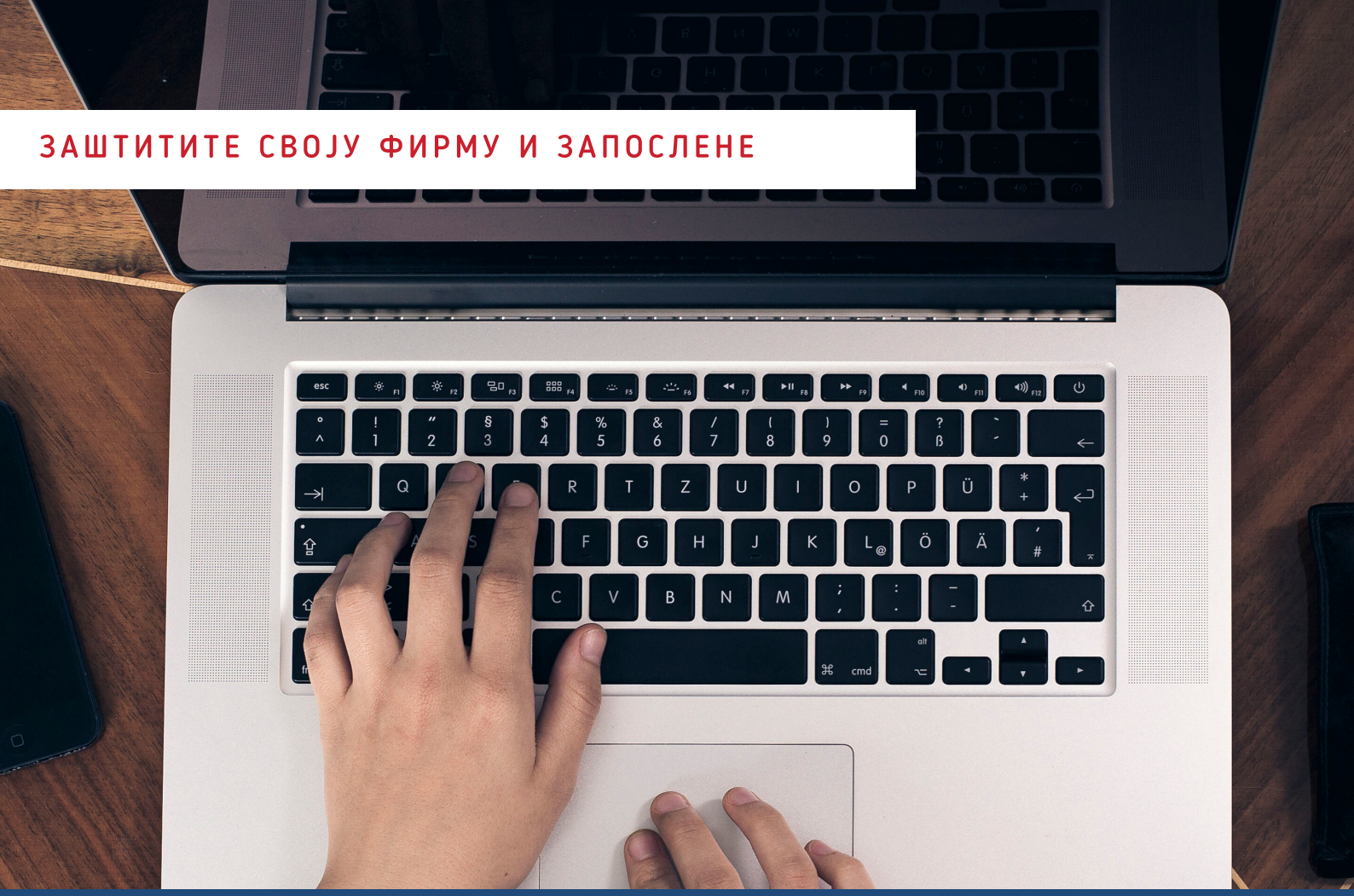
ЗАШТИТИТЕ СВОЈУ ФИРМУ И ЗАПОСЛЕНЕ



VPN ЗА МАЛА И СРЕДЊА ПРЕДУЗЕЋА

ПРИЈАВИТЕ СВАКИ ИНЦИДЕНТ
НА НАШЕМ ПОРТАЛУ

СРБ-ЦЕРТ

VPN

У данашње време, у погледу безбедности, како у приватном тако и у пословном окружењу, од највеће важности је заштита података и информација које размењујемо свакодневно путем интернета.

- Уколико се корисници налазе ван куће, у неком ресторану, хотелу, аеродрому или другом јавном месту, највећи број њих ће користити бежичне јавне тачке за приступ интернету, односно WiFi. Посматрано са безбедносног аспекта, највећи изазов представља сигурност коришћења оваквих приступних тачака, јер корисници немају увид ко све користи наведену тачку за приступ и да ли се надгледа и снима размена података путем те WiFi приступне тачке.

- Када говоримо о потреби корисника за радом на даљину, односно радом од куће, који подразумева приступање ресурсима software-as-a-service (SaaS), који припадају одређеној организацији или институцији, неопходно је да се такав рад обавља на безбедан начин, како не би дошло до могуће компромитације података којима корисник приступа.

- Како би корисници заштитили своје мрежне активности, приватност и спречили да дође до компромитације података организације препорука је коришћење виртуелне приватне мреже, односно VPN (енг. Virtual Private Network) приступ. VPN технологија креира приватни, шифровани тунел за активности на мрежи и знатно отежава било коме да прати или надгледа шта корисник ради док је на мрежи. Такође, VPN технологија омогућава компанијама бољу заштиту од могућег губитка и компромитације података, тако што се између корисничке мреже, било да се користи јавни или приватни WiFi, прави безбедан и шифрован тунел, преко јавног интернета до мреже организације.

ШТА ЈЕ VPN И КАКО РАДИ?

VPN је једноставан начин повезивања различитих мрежа које су одвојене од Интернета, користећи сигурносне протоколе који омогућавају аутентичност и поверљивост информација које путују VPN везом или мрежним системом.

- Апликације које се обично користе, било да су имејл, веб, поруке, друштвене мреже и сл, заснивају се на IP (Internet Protocol) протоколу. Иако су развијени одређени стандарди, нису све интернет апликације безбедне, одређен број апликација и даље није усаглашен са важећим прописима о начину дељења и заштите података. Неуједначен став о начину заштите података оставља простора могућим злоупотребама од стране нападача, односно хакера, који због оваквих пропуста једноставно могу доћи до личних података корисника, као што су број текућег рачуна, кредитне картице, кућне адресе и сл.

- VPN креира приватни тунел преко отвореног интернета. Идеја је да све што корисник пошаље буде енкапсулирано и шифрирано у овом приватном комуникацијском каналу, па чак и ако дође до пресретања послатих пакета, исти не могу бити дешифровани. VPN представља врло моћан и важан алат у заштити и безбедности корисника и њихових података, али има и своја ограничења. Овде се поставља питање ограничења VPN-а и разумевање где се налази крајња тачка VPN сервера. Уколико се корисник налази у Србији, а повезује се на VPN сервер у другој држави, целокупан саобраћај на интернету ће бити приказан као да је корисник приступио из мреже те друге државе, односно неће бити видљиво да је корисник приступио из IP опсега Републике Србије.

ТИПОВИ VPN-А

Два најчешће типа VPN-а су: корпоративни или пословни VPN сервис који представља пословно оријентисано решење које омогућава запосленима да се удаљено повежу на корпоративну мрежу и кориснички VPN сервис који појединцима омогућава да приватно сурфују од куће.

- Већина компанија има своје филијале или једнице које су географски удаљене, а повезивање таквих локација изнајмљеним приватним линијама може бити скупо, па их повезују путем јавног интернета, криптујући податке тако што користе корпоративни или пословни VPN. Корпоративни или пословни VPN карактерише иста организација која контролише обе крајње тачке VPN-а. Ако компанија контролише почетну тачку (рецимо продајну филијалу) и крајњу тачку (попут VPN сервера у вашем корпоративном седишту), можете бити прилично сигурни да се кориснички подаци сигурно преносе.

- Кориснички VPN користе они који често бораве на јавним местима, попут хотела, ресторана, аеродрома и сл, а повезују се на веб апликације попут друштвених мрежа, имејла, банака или веб страница за online куповину. Кориснички VPN сервис представља додатни вид заштите такве комуникације.

- Кориснички VPN сервис се у основи нуди софтвер као услуга (software-as-a-service - SaaS). VPN сервис пружа сигуран тунел између рачунарског уређаја (било лаптопа, телефона или таблета) и њиховог сервиса data центра. Важно је разумети да кориснички VPN сервис штите пренос података са локације корисника на њихову локацију, а не од локације корисника до одредишне апликације којој корисник жели да приступи.

- Овде су битне две ставке: Прва, уколико корисник приступа интернету користећи https протокол, те податке шифрује претраживач, а затим и VPN апликација. У VPN data центру подаци корисника се дешифрују само једном, а оригинална енкрипција коју нуди претраживач остаје неизмењена. Тако шифровани подаци се затим преносе на одредишну апликацију, попут банке корисника. Друга веома битна ставка је да веб апликација са којом корисник комуницира не види корисничку IP адресу. Уместо тога, она ће видети IP адресу која је у власништву VPN сервиса, а то кориснику омогућава одређени ниво анонимног умрежавања.

ИНСТАЛАЦИЈА VPN-А

Што се тиче пословног окружења, препорука је коришћење оних алата који се налазе у техничком оквиру и одобрени су од стране послодавца.

Управо из тог разлога, послодавац најчешће има унапред дефинисане техничке алате који запосленима омогућавају неометан и безбедан рад са удаљених локација, приликом коришћења службених лаптопова или мобилних уређаја. Овде се приоритетно мисли на коришћење firewall-а и антивирусне заштите, заједно са безбедносним функцијама као што су VPN и двофакторска аутентификација. Зашто је то важно: Алати послодавца који служе за безбедност дизајнирани су тако да заштите податаке и уређаје. Злонамерни корнисници (хакери) имају интерес да прикупе све расположиве типове података, било да радите у канцеларији или од куће. У пословном окружењу, ИТ администратор најчешће инсталира и подешава VPN, и креира одговарајуће упутство за коришћење VPN-а у складу са процедурама и политикама послодавца.

Када се ради о физичким лицима кориснички VPN сервис је веома једноставан за употребу. Први корак је проналажење одговарајућег VPN провајдера, а затим креирање налога (обично подразумева куповину њихове услуге). Након креирања корисничког налога, неопходно је преузимање, инсталирање и конфигурисање VPN софтвера, а затим се корисник повезује на интернет. Покретањем VPN софтвера, корисник креира шифровани тунел за размену података, који пружа одговарајућу заштиту.

Мрежне активности корисника су сигурне и остају приватне само уколико то обезбеди изабрани VPN провајдер. Препорука корисницима је да одаберу одговарајућег VPN провајдера у складу са својим потребама. Неке од кључних тачака приликом одабира одговарајућег пружаоца VPN услуга могу бити:

- **Логовање:** Одаберите услугу која не чува логове и фокусирана је на приватност. Уколикопружалац VPN услуге не сакупља никакве логове, много је теже да неко претражи и увиди шта је корисник радио док је био на мрежи.
- **Где је основана компанија:** Различити VPN провајдери пружају своје услуге корисницима широм света. Препорука је да корисници изаберу VPN провајдера са седиштем у оним државама које имају добро развијене законе о заштити података. VPN провајдери смештени у земљама које имају слабе законе о приватности могу бити приморани да дају информације које прикупе о корисницима.
- **Сервери:** Одаберите VPN услугу која има сервере у земљама или градовима који одговарају вашим потребама. Неки VPN провајдери имају велики број сервера и локација широм света. Све наравно зависи од потреба корисника, а ту се поставља питање: Да ли корисник има потребу да везе које успостављa изгледају као да долазе из одређене земље? Да ли VPN провајдер може то да пружи?
- **Компатибилност:** Пронађите пружаоце услуге који раде на различитим оперативним системима и мобилним уређајима. На пример, корисник може имати Windows оперативни систем на лаптопу, Андроид таблет и iPhone мобилни телефон, и потребу да VPN услуга ради на свим тим уређајима.
- **Избегавајте бесплатне услуге:** Будите веома опрезни према „бесплатним“ VPN услугама. Поставља се питање на који начин такви VPN провајдери зарађују новац и остају у послу? Пружаоци бесплатних услуга могу прикупљати и продавати податке корисника, тако да је важно обратити пажњу на услове које нуде.

КАДА ЈЕ ПОТРЕБНО КОРИСТИТИ VPN?

Када се ради о пословном окружењу, већ је напоменуто да сваки пут када су географски удаљене локације (било да је у питању рад од куће или друга филијала) које треба да се повежу преко јавног интернета, треба размислити о коришћењу VPN технологије, која кориснику може помоћи да заштити размену података током рада од куће или са друге локације.

- VPN пружа сигурну везу између запослених и послодавца шифровањем података и скенирањем уређаја на злонамерни софтвер попут вируса, рансомвера и сл. У том случају ће VPN софтвер вероватно бити покренут на рутеру, серверу или наменском хардверском уређају за VPN сервер.
- Веома је важно да корисник укључи VPN када ради од куће или са друге удаљене локације и приступа подацима или размењује битне пословне информације. VPN омогућава заштиту од злонамерних корсника (хакера) и онемогућава им да виде шта корисник ради на мрежи током радног дана, што укључује слање или примање финансијских информација, стратешких докумената и података о клијентима. VPN помаже да се те информације сачувају од злонамерних корсника (хакера), али и конкурената.
- Када се корисник који ради ван куће или канцеларије, повезује се на интернет, најчешће путем WiFi мреже која је у власништву хотела, ресторана, аеродрома или друге јавне установе. У овим ситуацијама, корисник нема сазнања ко још користи исту приступну тачку бежичним интернету и самим тим може доћи до злоупотребе путем пресретања саобраћаја на мрежи. Препорука Националног ЦЕРТ-а је да корисник увек када је ван канцеларије или куће, а користи туђу WiFi мрежу (чак и члана породице или пријатеља, јер немате сазнање да ли су били угрожени), користи VPN. Посебно је важно уколико корисник приступа услугама које захтевају личне податке. Имајте на уму да се много тога догађа иза сцене што није видљиво, а никад се заправо не зна да ли једна или више корисничких апликација потврђују аутентичност у позадини и доводе податке у ризик.

ПРЕДНОСТИ И НЕДОСТАЦИ VPN-А

ПРЕДНОСТИ

- **Побољшава безбедност.** Када се корисник повеже на мрежу путем VPN-а, подаци се преносе путем безбедног и шифрованог тунела. На овај начин су информације заштићене од сваког ко покушава да приступи личним подацима и другим подацима које том приликом корисник размењује.
- **Удаљени приступ.** У случају компанија, велика предност поседовања VPN-а је та што се информацијама може приступити удаљено, од куће или са било ког другог места. На овај начин VPN може повећати продуктивност компаније.
- **Анонимност на мрежи.** Кроз VPN корисник може сурфовати интернетом потпуно анонимно. У поређењу са скривањем IP адреса путем софтвера или веб проксија, предност VPN услуге је та што кориснику омогућава приступ веб апликацијама и веб страницама потпуно анонимно. Приватност се штити тако што се маскирају информације попут IP адресе, локације и историје претраге, како их не би пратили веб сајтови, интернет претраживачи и други.

- **Боље перформансе.** Ширина пропусног опсега и ефикасност мреже се обично могу повећати након примене VPN решења.

- **Смањује трошкове.** Једном када се креира VPN мрежа, трошкови одржавања су врло ниски. Штавише, ако корисник одабере провајдера сервиса, подешавање мреже и надзор нису више брига корисника.

ПРЕДНОСТИ И НЕДОСТАЦИ VPN-А

НЕДОСТАЦИ

- **Најбољи VPN-ови, нису беспалтни.** Пружаоци бесплатних услуга могу прикупљати и продавати ваше податке, јер се поставља питање на који начин зарађују. Већина њих не користи шифровање или нису правилно конфигурсани, а на тај начин приватност корисника на интернету је угрожена и постоји могућност да злонамерни корисници пресретну саобраћај и дођу у посед корисничких података. Такође, неки бесплатни VPN-ови могу да корисника изложе злонамерном софтверу, продају пропусни опсег ботнетима или чак прикупљају личне податке и продају их оглашивачима или трећим странама. На крају, уколико корисник жели да подаци буду сигурни, неопходно је платити поуздану VPN услугу.

- **VPN-ови изворно не раде на свим платформама.** VPN-ови обично раде на најпопуларнијим уређајима и оперативним системима, али још увек постоје неке платформе које немају њихову подршку, као што су неки типови паметних телевизора, конзоле за играње (Xbox, PlayStation) и сл. У том случају неопходно је да корисник постави VPN везу на рутер, што може бити прилично сложен процес и на тај начин сваки уређај приступаће интернету путем тог рутера користећи VPN који је креиран. Алтернативно, VPN везу корисник може делити и путем рачунара или лаптопа повезивањем уређаја са етернет каблом. Међутим, оваквим повезивањем корисник може успорити перформансе мреже или смањити проток, а додатни изазов представља повезивање већег броја уређаја путем рачунара или лаптопа.

- **Коришћење VPN-а може смањити брзину везе.** Један од главних недостатака VPN услуге са којим корисници имају проблем јесте смањена брзина везе. Иако се то не догађа сваки пут када корисник користи VPN за приступ интернету, брзина мреже се некад може успорити, а то се обично дешава у следећим случајевима: када је шифровање прејако, VPN протокол који корисник употребљава није оптимизован за брзину и зато што је удаљеност између VPN сервера који корисник користи и корисничког уређаја превелика. Наравно, постоје и други фактори који могу утицати, али то су најчешћи разлози због којих се брзина везе може мало успорити када користите VPN.

- **Неки VPN-ови сакупљају корисничке податке.** Неки провајдери VPN услуга сакупљају корисничке податке, најчешће су то информације о њиховој конекцији, али понекад могу сакупљати и чувати личне податке. Већина провајдера то ради како би се придржавали закона својих земаља. Иако је то разумљиво, VPN који сакупља и чува корисничке податке, прилично утиче на основну идеју употребе VPN-а, а то је итегритет података. Овај проблем се може избећи уколико се одабере VPN провајдер који има строгу и јасну политику која не сакупља и не чува податаке или провајдера са седиштем у земљи која има јаке законе о приватности.

ЗАКЉУЧАК

VPN је најбољи начин да се заштити приватност корисника на мрежи.

- Међутим, VPN не ради ништа на обезбеђивању рачунара, уређаја или мрежних налога. Чак и ако корисник употребљава VPN, битно је да увек следи основне мере заштите, укључујући редовно ажурирање уређаја, закључавање екрана и коришћење јаких, јединствених лозинки за све корисничке налоге.

Извор:

- 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/

РЕПУБЛИКА СРБИЈА
РАТЕЛ
РЕГУЛАТОРНА АГЕНЦИЈА ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ И ПОШТАНСКЕ УСЛУГЕ

СРБ-ЦЕРТ