Wat is een VPN?

En wat doet het?

Rein de Jong

Een Virtual Private Network (VPN) biedt een veilige en beschermde netwerkverbinding over het internet, tussen een computer of mobiel apparaat en een ander apparaat.
Je echte IP-adres wordt verborgen en er wordt je een nieuw, tijdelijk adres verstrekt door de VPN-aanbieder. VPN-providers hebben over de hele wereld servers staan, die je in praktisch elk land waar je dat wilt een lokaal IP-adres kunnen verstrekken.

Verzet tegen verzamelwoede

Op zijn laatste concert, vlak voor zijn overlijden, zong Udo Jürgens in 2014 het lied *'Der gläserne Mensch'*[1]. Zoals veel Duitsers was Udo Jürgens er al van doordrongen dat we als gewone burgers blootstaan aan de verzamelzucht van overheden en techbedrijven. Het Duitse dorp Molfsee verzette zich met succes tegen de verzamelwoede van Google Street View. Veel plaatsen in Duitsland volgden.

Kijk je met Street View naar de grotere plaatsen in Duitsland, en kies je bijvoorbeeld Berlijn, dan zie je veel verhulde gebouwen. Daarom wordt Duitsland regelmatig *'Blurmanie'* genoemd. Daaruit blijkt dat ook jij je prima kunt verzetten tegen de opslag van jouw bezit[2]. Een ander middel waarmee je jezelf kunt verhullen voor de verzamelwoede van overheden en bedrijven is een Virtueel Privé Netwerk (VPN).

Wifi In het buitenland

Tijdens je vakantie op een mooie plek in Hongarije maak je graag gebruik van het daar geboden wifi-netwerk. Je gebruikt het om je mail te lezen, informatie op te zoeken en misschien wel om contact te zoeken met je bedrijf of overheidsinstellingen, zoals het UWV. Daarnaast doe je ook al je betalingen die nodig zijn tijdens je vakantieperiode. Je bent verbaasd dat je geen toegang krijgt tot het netwerk van je werkgever en ook kun je de laatste afleveringen van *'Orange is the new Black'* op Netflix niet zien.

Onbeveiligde hotspot

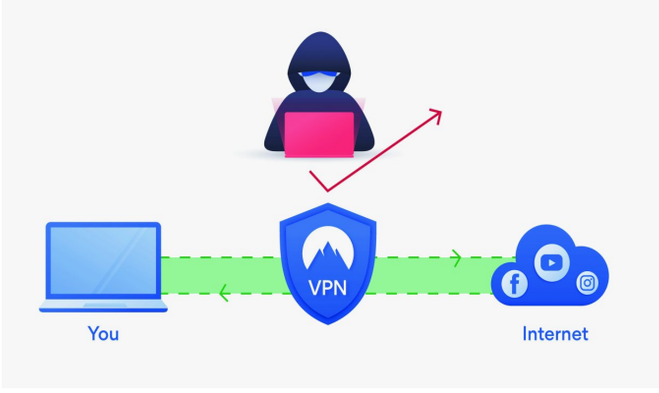
Een vrouw werkt zakelijk op haar laptop en mobieltje in een café of flexwerkplek en maakt verbinding met de wifi-hotspot. Ze gebruikt de onbeschermde hotspot om te werken aan een nieuw ontwerp voor kleding, te winkelen, te mailen met haar opdrachtgever en haar rekening te betalen. Ondertussen zit een jongeman rustig in een hoek van de zaal, is ongestoord bezig op zijn laptop, neemt af en toe een slok van zijn koffie en kijkt dan weer in een tijdschrift waarbij hij de zaal ongemerkt in ogenschouw neemt. Zij weet niet dat haar gebruik van de internetverbinding door hem wordt gevolgd. Daarbij wordt waardevolle persoonlijke en zakelijke informatie gestolen. De vrouw is dan ook zeer verbaasd wanneer zij enkele weken later de door haar ontworpen jurk bij een concurrent ontdekt.

Een burger, woonachtig een land dat door een totalitair regime wordt geregeerd, wil websites kunnen bezoeken om onafhankelijke berichtgeving te kunnen volgen en zich op forums begeven waar mensen met kritiek op het regime zich verzamelen. De overheid blokkeert deze websites echter uit 'veiligheidsoverwegingen'.

De voordelen van VPN

Bovenstaande situaties zijn schoolvoorbeelden van problemen die met een Virtual Private Network (VPN) kunnen worden opgelost. Jouw gegevens die over het netwerk gaan worden door VPN beschermd. VPN geeft je toegang tot websites, forums en diensten die normaal gesproken niet vanaf jouw verblijfplek bereikbaar zijn. Die toegangsbeperkingen kunnen een gevolg zijn van censuur van de overheid, maar kunnen ook het gevolg zijn van het afschermen van tv- en video-aanbod dat wel beschikbaar is in landen waar het aanbod online is geplaatst, zoals Nederland of de VS, maar niet in andere landen. Daarnaast maakt VPN het voor advertentienetwerken moeilijker je te volgen.

Een VPN versleutelt de gegevens die jij over het netwerk stuurt. Of dat nu een intern netwerk of het wereldwijde internet is maakt niet uit. VPN legt een veilige schil rondom de door jou verzonden en opgevraagde gegevens en daardoor zijn ze veilig voor de ongewenste blikken van overheden en bedrijven.

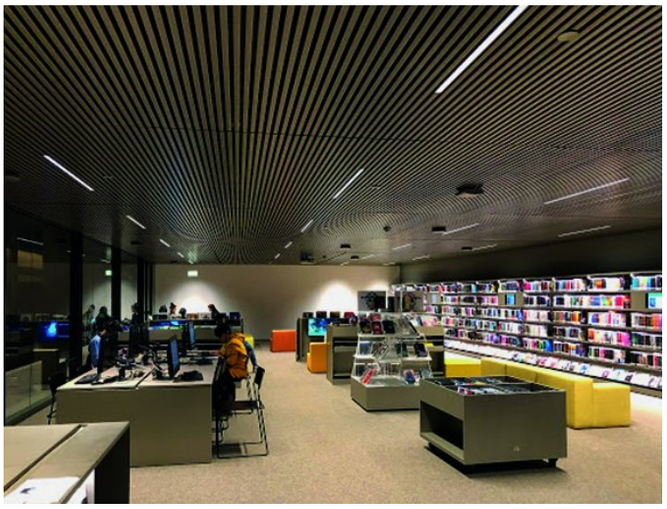


VPN biedt je privacy, veiligheid en vrijheid.

Voor het opzetten van een VPN-verbinding is een ander apparaat nodig, een server, die je beveiligd toegang geeft tot webdiensten die mogelijk niet vanaf je eigen locatie beschikbaar zijn en daarnaast legt het een beschermingslaag over de daadwerkelijke verbinding. Zie dat maar als een afgeschermde tunnel waardoor jouw gegevens heen-en-weer gezonden worden.
Vanaf jouw apparaat, of dat nu een pc, tablet of smartphone is, zet je eerst een punt-naar-punt verbinding op met de VPN-server. Vandaaruit ga je dan, via een eveneens beveiligde verbinding het Internet op. Internet ziet de VPN-server dan als de klant. De VPN-server fungeert als een soort beveiligd doorgeefluik voor jou.

Waarvoor gebruik je een VPN?

Dat we weten wat een VPN inhoudt, wil nog niet zeggen dat we weten wat er mee te doen. Alleen dat het een oplossing is voor de drie voorbeelden zoals genoemd in de inleiding. Omdat we zo'n situatie vóór willen zijn kan ik wel stellen dat een VPN iets is wat je zou moeten hebben. Ik heb het dus wel!



Je kunt het gebruiken om veilig te bankieren of een veilige verbinding op te zetten met je werk, al is het maar voor het gebruik van Facebook. Het voorkomt dat je netwerkverbinding wordt gemonitord. Een VPN stelt je in staat om het internet anoniem en in alle vrijheid te gebruiken zoals het oorspronkelijk is bedoeld, zonder restricties die zijn opgelegd door de je Internetprovider of de overheid. Het voorkomt ook dat je provider je surfgedrag vastlegt zoals die volgens de sleepwet verplicht is te doen. Kortom, het geeft je veiligheid, privacy en vrijheid.

Een VPN stelt je in staat om:

1. Een veilige verbinding op te zetten met je werkomgeving
   Werkgevers die bewust met veiligheid omgaan dwingen dit al af bij hun werknemers. Voor thuiswerkers is het gebruik van VPN een must. VPN-verbindingen zijn in het bedrijfsleven gemeengoed en ze lopen daarin voor op de privé-gebruiker. Wordt het nog niet geboden? Dring er dan bij de werkgever op aan een veilige VPN-server te installeren. Het is de enige manier om het intellectueel eigendom te beschermen tegen kwaadwillende afluisteraars.
2. Onderweg veilig op internet te werken
   Wanneer je onderweg bent en via een ongecontroleerde wifi-toegang werkt, denk hierbij aan publieke ruimtes zoals horeca, campings en gezondheidsvoorzieningen gebruik dan VPN. Gebruik je de wifi van een bekende, dan zou VPN overbodig kunnen zijn.
   Gebruik je een eigen mobiel netwerk, al dan niet via een Hotspot, ook dan is VPN voor de veiligheid niet per se nodig.
3. Vanuit huis je verbinding af te schermen van monitoring
   Stel: je wilt dingen doen die je wenst te verhullen. Dat hoeven geen illegale zaken te zijn, maar denk hierbij aan het zoeken naar informatie over gezondheidsproblemen of beleggingen. Dat zijn privacy gevoelige onderwerpen die je niet in het sleepnet van de overheid wenst. Je weet immers niet wat zij er nu of in de toekomst mee gaan doen en de wettelijke bewaartermijn wordt sowieso overschreden, getuige de vele onderzoeken die worden gepubliceerd. Ook dan kun je overwegen om vanuit huis een VPN op te zetten en daar de acties te doen die je wenst te verbergen. Wanneer je anoniem wilt deelnemen aan discussies op forums en Social Media is VPN ook een uitkomst. Je verstopt jezelf voor je provider, de overheid en de adverteerders. Een VPN is zo een aanvulling op het gebruik van een veilig ingestelde browser.
   Zelfs wanneer een vreemde toegang heeft tot jouw netwerk, een hacker of iemand die jij in vertrouwen toegang tot jouw netwerk geeft, beveiligt een VPN jouw verkeer door het via de beschermende tunnel te leiden.
4. Censuur te vermijden en geeft toegang tot locatieafhankelijke content
   Wanneer je je kunt voordoen als afkomstig uit een ander land, dan kun je inhoud zien, die alleen bedoeld is voor dat land. Denk aan series die in de VS al wel beschikbaar zijn maar nog niet in Nederland. Of vanaf je vakantieadres een Nederlandse VPN kiezen die je dan toestaat om inhoud van Ziggo, NPO en andere streamingservices te zien die anders als verzoek vanaf een buitenlands adres worden geblokkeerd.
   Je kunt je in een land bevinden met een totalitair regime zoals China, waar internetcensuur wordt toegepast, dan zou je zomaar kunnen merken dat je niet meer op je vertrouwde websites kunt komen omdat die door de overheid worden geblokkeerd. Die regimes trachten ook VPN-servers te blokkeren. Daar zul je bij het selecteren van een aanbieder rekening mee moeten houden. VPNmentor geeft uitleg over hoe je deze blokkades kunt omzeilen[3].
5. Anonieme toegang te verkrijgen tot torrent- en P2P-sites
   Er zijn internetproviders die blokkades opwerpen ten aanzien van torrent- en P2P sites; de overheid verbied KPN, Ziggo en XS4all om je toegang te geven tot *'thepiratebay'*. VPN kan je helpen dat te omzeilen.
   Weinig mensen erkennen dat ze gebruik maken van torrent- en P2P-sites en toch is het vaak de hoofdreden waarom een VPN wordt benut; juist om anoniem bij content te komen waartoe je normaal geen toegang hebt of voor illegaal downloaden. Besef wel dat illegaal gedownloade content zo maar een *'Paard van Troje'* kan zijn waardoor je zelf ongewenste sujetten toelaat; wees dan ook niet verbaasd wanneer je eigen data zomaar versleuteld is. Alleen een goede back-up biedt dan uitkomst. Maar je kunt ook toegang tot torrentsites wensen voor volkomen legale doelen om met behulp van een .torrent grote bestanden op te halen. Wanneer een ISP de bandbreedte voor torrents afknijpt kan VPN een oplossing zijn.

Hoe veilig is VPN?

Met behulp van een aantal veilige algoritmes (protocollen genoemd) wordt een veilige tunnel gecreëerd tussen jou en het internet. Het netwerkverkeer wordt door het protocol zodanig versleuteld dat het afluisteren van jouw verbinding alleen maar een brei oplevert van nullen en enen waar geen touw aan vast te knopen is. Allerlei slimme analyseprogramma's kunnen alleen maar zien dat het versleutelde data is. Kraken kan, maar dat vergt veel tijd en inspanning; zo lang dat het jaren kan duren voordat de verbinding is ontsleuteld.

Er is een groot aantal verschillende protocollen[4]; die ga ik hier niet beschrijven. De link geeft je uitleg en je kunt daarin net zover gaan als je belangstelling reikt.
Het veiligste protocol is *OpenVPN* en het daaraan verwant *OpenSSL*. Biedt een VPN-client dat, kies het dan. Het heet niet voor niets: **Open**XXX. Beide maken gebruik van open-source technieken die openbaar zijn en dus gecontroleerd kunnen worden op achterdeurtjes. *Wireguard* is een nieuw experimenteel open-source protocol dat ook nog erg snel en veilig is, maar net als OpenVPN en OpenSSL nog niet breed wordt ondersteund.
Daarnaast zijn er nog in volgorde van veiligheid de protocollen *SSTP* en *L2TP/IPSec*. Het verouderde *PPTP* zou je moeten vermijden, maar het is beter dan niets.

Een VPN-provider kiezen?

Waar moet je op letten bij de keuze voor een VPN-aanbieder? Je zult jezelf vragen moeten stellen: wat wil je van de VPN-verbinding, zoals de snelheid, het bijhouden van logboeken, wordt een onafhankelijke audit toegestaan, het aantal landen waar hun servers zich bevinden en de beschikbaarheid daarvan, de aangeboden protocollen, of torrents zijn toegestaan, enzovoort. Een van de belangrijke aspecten is privacy; staat een VPN-aanbieder een audit toe; zijn er voorbeelden van VPN-providers die de overheid geen logboek willen - of nog beter niet kunnen overhandigen. Niet onbelangrijk is de vraag hoeveel je wilt of kunt betalen? Nu we het toch over betalen hebben, het is minstens zo belangrijk wanneer je anonimiteit wenst, dat je ook anoniem kunt betalen.

Er zijn providers die volledig gratis zijn, maar dan is jouw data de prijs die je betaalt. Ik ben dan ook terughoudend in het aanbevelen van gratis mogelijkheden. Sommige goede providers bieden ook volwaardige gratis varianten aan voor sporadisch gebruik. Ben je in het bezit van een modem zoals bijvoorbeeld de Fritz!Box, dan kun je die als VPN-server gebruiken om vanaf een buitenhuislocatie veiliger te kunnen werken. Je hebt dan vanaf een buitenlands adres toegang tot Nederlands gelokaliseerde content en tevens een veilige toegang tot je thuisnetwerk.
Er zijn vele testen van VPN-providers te vinden, zoals die van PCMweb[5]. Bij veel testen komt *ExpressVPN* als een van de beste uit de bus.

Mijn Keuze

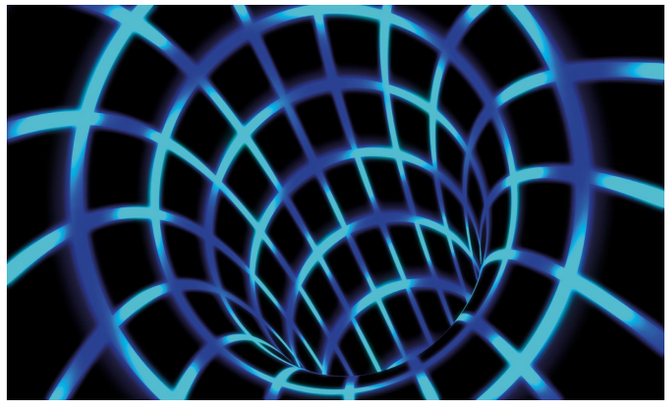
Gelet op het feit dat ik een Fritz!Box als router bezit zet ik die in als VPN-server wanneer ik van huis ben. Wil je zelf ook je Fritz!Box als VPN-server inzetten? Lees dan op de site van AVM[6] hoe je dat doet.
Voor de enkele keer dat ik mij anoniem op het internet wil bewegen, maak ik gebruik van VPN Unlimited. Ik kon via **wccftech**[7] voordelig een 'levenslang' abonnement afsluiten. Op de site van **wccftech**[7] staan nog regelmatig aanbiedingen voor *VPN Unlimited*. Een test van VPN Unlimited lezen? Dat kan op de site van **VPNmentor**[8].

Heeft VPN ook nadelen?

Natuurlijk kleven er ook nadelen aan het gebruik van een VPN-server. Het is gedoe en het kost geld. Een aantal VPN-servers wordt als malafide aangemerkt waardoor je van sommige diensten wordt geweerd.

Het gebruiken van een VPN is trager dan een directe verbinding. Je bent immers afhankelijk van de snelheid die de VPN-server je biedt. Alle VPN-aanbieders vertragen je verbinding. Dat is inherent aan het maken van een omweg. Uit testen blijkt dat de goede providers je niet meer dan tot 70% van je eigen snelheid verlagen.

De vraag is in hoeverre de nadelen, de kosten en de vertraging opwegen tegen de hier geschetste voordelen.



Links

1. Der gläserne Mensch — https://bit.ly/r-dgm
2. Mijn huis van Streetview — https://bit.ly/r-hvs
3. VPN-blokkade omzeilen — https://bit.ly/r-vpnomz
4. VPN-protocollen — https://bit.ly/r-vpnp
5. Test VPN-aanbieders — https://bit.ly/r-vpntst
6. Fritz!Box VPN-server — https://bit.ly/r-fbvpn
7. VPN Unlimited Lifetime — https://bit.ly/r-vpnunl
8. Test VPN Unlimited — https://bit.ly/r-vpnt

Mijn andere artikelen — https://bit.ly/r-art