SECURITY & AVG

GOOSE VPN: VEILIG WERKEN MET MOBIELE APPARATEN

Ideale beveiligingsoplossing voor ambulante medewerkers

In de moderne samenleving zijn er twee trends die de toon zetten: het steeds mobieler worden van medewerkers en het steeds grotere belang van IT in de bedrijfsprocessen. Was het op locatie werken met een laptop voorheen vooral weggelegd voor bijvoorbeeld vertegenwoordigers, vandaag de dag krijgt elke medewerker min of meer standaard een laptop in plaats van een vaste pc.

tekst Hans Steeman

Vierentwintig uur per dag zeven dagen per week toegang tot de bedrijfsomgeving is eerder regel dan uitzondering. Een laptop staat flexwerken toe en is overal inzetbaar, een smartphone of tablet is daarnaast ook nog extra flexibel. Wifi, het draadloze ethernet, is daarbij een onlosmakelijke noodzakelijk. Een stap verder is het gebruik van mobiele apparaten zoals telefoons en tablets via een mobiel netwerk. Dankzij deze portable computers in pocketformaat is elke IT-omgeving feitelijk overal waar wifi of een mobiel netwerk beschikbaar is te benaderen. Hierdoor kunnen bijvoorbeeld thuiszorgmedewerkers als ze een patiënt bezoeken, de laatste medische informatie raadplegen en het zorgdossier bijwerken. Alles is dan direct vastgelegd en geadministreerd. Het mobiel worden van IT heeft ontegenzeggelijk de efficiency van bedrijven verhoogd, en bijna geen enkele organisatie kan binnenkort nog zonder een mobiele IT-oplossing.

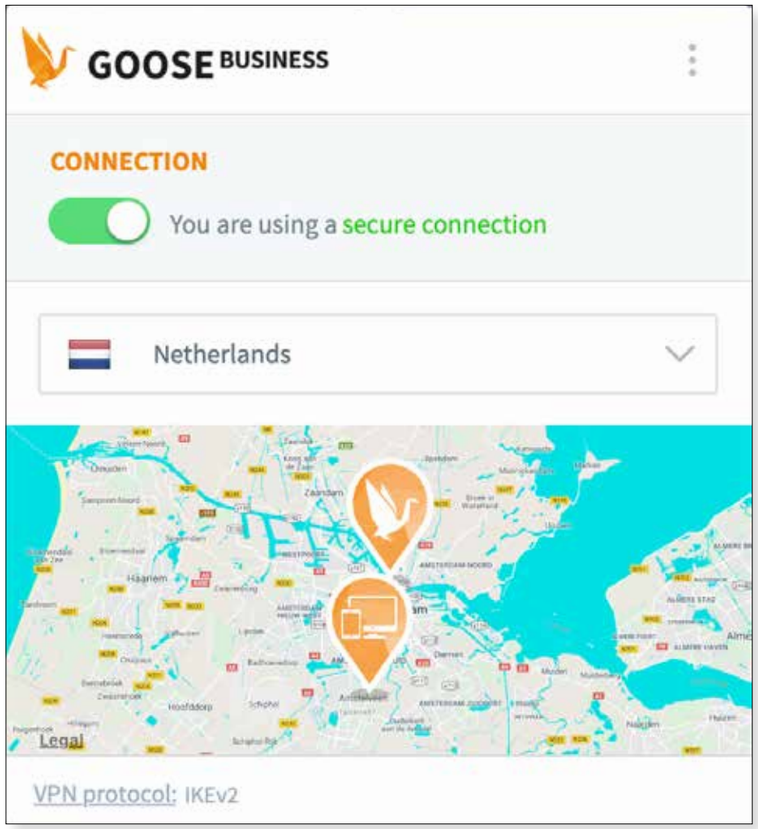
Een VPN geeft een veilig gevoel

Hier ligt dan ook de kern van het succes van Goose VPN, de Nederlandse VPN-provider bij uitstek. Zij hebben met hun VPN-oplossing de sleutel in handen om het mobiel gebruik van privacygevoelige informatie absoluut veilig te maken, zonder dat de gebruiker er op enige wijze iets van merkt. Joeri van de Watering: “Wij zijn trots om als relatief jonge onderneming al zoveel waardevolle zakelijke klanten onze diensten te kunnen leveren. Het geeft aan dat veiligheid bij steeds meer bedrijven hoog in het vaandel staat. Zeker met de aangescherpte GDPR/AVG wet- en regelgeving is het gebruik van een beveiligde internetverbinding een noodzaak. Het verloren gaan van privacygevoelige gegevens is zo ongeveer het ergste dat een bedrijf kan overkomen. De sancties zijn erg groot.”

> ‘Wij zijn op zoek naar gepassioneerde channelpartners die met ons willen samenwerken’

Mobiele werknemers staan aan veel risico’s bloot, zonder het vaak zelf te realiseren. Zodra men met een computersysteem of smartphone in een publiek wifi-netwerk terechtkomt – dat kan al gebeuren als men op straat rondloopt of een hotel, winkel of restaurant bezoekt – legt het apparaat veelal ongemerkt contact met het open wifi-netwerk en daarmee het internet. Een ‘man in the middle attack’, een situatie waarbij iemand tussen het apparaat en het internet een tussenstation creëert, is dan erg groot. Alle data kan bij een niet versleutelde verbinding onderschept worden. Accountinformatie, username en password, ligt dan, voor men het zich realiseert, op straat. Het is geen theoretisch risico, er zijn veel voorbeelden van zulke incidenten bekend. Gratis wifi is als een honingpot voor de moderne prijsbewuste mens. Bij een goed opgezette aanpak van de hacker, heb je niet eens in de gaten dat je een risico loopt. Als iemand snel even een publiek wifi-netwerk gebruikt om bijvoorbeeld e-mail te raadplegen kan het al gebeurd zijn.

Joeri van de Watering: “Onze VPN kan dan voor een goede bescherming zorgen, niemand heeft toegang tot de dataverbinding (versleuteld met naar keuze IKEV2 en IPsec tussen beide eindpunten). Al het verkeer is volgens de meest geavanceerde encryptie beveiligd, en een geïntegreerde ‘kill switch’ verbreekt automatisch de verbinding als de VPN ineens wegvalt.



Nieuw is dat we nu ook zogenaamde trusted verbindingen, op basis van een vertrouwd netwerk, kunnen ondersteunen.” Vertrouwde netwerken zijn bijvoorbeeld het zwaarbeveiligde bedrijfsLAN of de internetverbinding van de mobiele operator. Op dit soort netwerken is een ‘man in the middle’ principieel niet mogelijk. De nieuwe Goose VPN kan dit soort verbindingen automatisch herkennen en er zijn policy op aanpassen.

Alles inclusief

Goose VPN is een mobiele VPN-oplossing die geschikt is voor Mac OSX, Windows, Chrome, Linux, iOS en Android en werkt ook in routers. Elk mobiel apparaat en infrastructuur is er dus mee te beveiligen. In een pull-downmenu van de app zijn meer dan 20 landen en meer dan 80 servers te selecteren waar de verbinding getermineerd wordt. Zakelijke gebruikers hebben zelfs nog wat extra serveropties, allemaal met één simpele click.

Van de Watering: “Onze Nederlandse afkomst geeft extra vertrouwen. We handhaven ons perfect tussen het grote aanbod van buitenlandse VPN-providers. Wij zijn een 100 procent Nederlands bedrijf; dit speelt zeker mee in het keuzeproces van onze klanten. Alle data loopt uiteindelijk via onze servers, vertrouwen is daarom ontzettend belangrijk. Ik begrijp goed dat men daarom liever voor een Nederlandse oplossing kiest dan de oplossing van een bedrijf zonder gezicht en gevestigd op een tropisch paradijs.”

Uitbreiding is gewenst

Nu Goose VPN als mobiele VPN-oplossing gefinaliseerd is en de gebruikers tevreden zijn, ontstaat er behoefte aan expansie. Daarbij is er plaats voor channelpartners. Met het product kunnen zij op snelle en efficiënte wijze de zakelijke klanten te hulp schieten bij het beveiligen van hun IT-omgeving. Joeri van de Watering: “Wij zijn op zoek naar gepassioneerde channelpartners die met ons willen samenwerken. Wij bieden een degelijk product met een Nederlandstalige helpdesk en een mooie marge. Daarmee hebben channelpartners een betrouwbare partner erbij.” «

Een welgemeende raad

Ook een organisatie als Interpol (de overkoepelende internationale organisatie van de politie voor de aanpak van criminaliteit), raad aan om een VPN te gebruiken, zowel privé als zakelijk. Een toenemende trend is dat ook binnen bedrijven het management wordt gehackt door medewerkers en ex-medewerkers. Het is helaas vrij eenvoudig om een hack uit te voeren. Google even ‘How to hack WIFI wireless Network’ en na het bekijken van een YouTube-video ben je zo goed als klaar om de hack te doen. Nog even wat hardware bestellen voor 80 euro en klaar is Kees. Veel van de hacks zijn vrij onschuldig, medewerkers die nieuwsgierig zijn waar het management het over heeft. Maar het komt ook voor dat het overgaat in afpersing... Reden genoeg om een VPN serieus te overwegen.

https://goosezakelijk.nl zakelijk@goosevpn.com 085 303 6195