#KLOOIENMETCOMPUTERS

ARNOUT VAN KEMPEN OVER ROMMELEN IN EEN DIGITALE WERELD

Het internet is ontstaan uit Amerikaanse militaire en universitaire initiatieven, in een tijd dat de grootste zorg was dat de Russen ieder moment een atoombom konden gooien. Het is dan ook extreem goed bestand tegen vernietiging van grote delen van de infrastructuur. Alle data wordt in pakketjes het net op gestuurd en die pakketjes zoeken een beschikbare weg naar hun doel. Daar aangekomen worden pakketjes weer samengevoegd tot het oorspronkelijke bericht. De data die je verzendt, kan daarbij vele knooppunten passeren. En in de basis is die data niet versleuteld.

Het is goed te bedenken dat ieder pakketje zowel zijn doel als zijn bron kent en dat de knooppunten die de pakketjes doorsturen gewone computers zijn; bijvoorbeeld van de naburige universiteit, van Amazon of van de Chinese overheid. Dit systeem is snel en onwaarschijnlijk robuust. Maar zonder maatregelen volstrekt onveilig voor twee zaken:

1. Al je data kan worden gelezen door iedereen met toegang tot een knooppunt.
2. Zowel jij als je geadresseerde zijn extreem eenvoudig te vinden.

Encryptie kan het eerste probleem oplossen, maar het tweede niet. En het is niet onbelangrijk te bedenken dat heel veel internetverkeer geen gebruikmaakt van encryptie. Wie op het wifinetwerk van het vliegveld of de camping nog snel even wat zakelijke mails bekijkt of een dossier afsluit voor vakantie, is extreem kwetsbaar, want het wifinetwerk zit vóór het eerste internetknooppunt. Dus wie meeluistert krijgt zonder probleem alle pakketjes data, op volgorde, gepresenteerd. Wie dat eens wil uitproberen moet op zoek naar een *sniffer*. Google is je vriend hier.

Hoe los je zowel het wifiprobleem als het probleem van adressering op? Met een VPN, een *virtual private network*. Dat is in de basis een bedrijf dat over de hele wereld computers heeft staan die doen alsof ze jouw computer zijn. Jij stuurt je data, *encrypted*, naar een van de VPN-computers en de VPN-computers sturen jouw bericht, alsof het van henzelf is, naar het doel. Resultaat: Jouw communicatie met de VPN-computer is encrypted en zodra je datapakketjes daadwerkelijk het internet opgaan, zien ze eruit alsof ze van die VPN-computer zijn. Jij bent onzichtbaar geworden, je locatie is die van de VPN-computer geworden. En dat kan dus iedere locatie op de planeet zijn. Handig, als je bijvoorbeeld een kritische blog over China schrijft vanuit Hong Kong en de overheid ziet dat je berichten uit Timboektoe komen. Maar ook handig als je vertrouwelijke mails met klantinformatie verstuurd en niemand kan ze meelezen, ook niet op de camping.

Een VPN is gratis, een goede VPN kost geld. Een heel goede VPN kost zelfs behoorlijk wat geld. Zelf gebruik ik ExpressVPN voor ruim honderd euro per jaar. NordVPN, dat van vergelijkbare kwaliteit is, kent vergelijkbare prijzen. Wat zijn zo wat voordelen van een goede VPN? Veel servers over de hele wereld, hoge snelheid, betrouwbaarheid, natuurlijk. Maar ook de zekerheid van een *killswitch* die jouw verbinding direct verbreekt als het systeem om welke reden dan ook ziet dat de VPN-verbinding uitvalt. Gebruik van *ramdrives*, zodat als een overheid de VPN-servers opeist, deze leeg zijn zodra de stroom er af gaat. Vestiging in een obscuur land dat niet deelneemt aan verdragen waardoor de overheid informatie kan opeisen.

Persoonlijk vind ik een goede VPN onderdeel van de basishygiëne van iedereen die online gaat met vertrouwelijke data. Dat wil overigens niet zeggen dat het altijd nodig is. Maar zeker als je zelf verantwoordelijk bent voor dit soort zaken, als zzp'er bijvoorbeeld, is het wel iets waarin je je zou moeten verdiepen. ←