Sinds er veel via internet gaat, is het veel makkelijker geworden om in contact te komen en te blijven met gelijkgestemden. Ook is het veel makkelijker om acties aan te kondigen. Dat weten de overheidsdiensten AIVD en MIVD echter ook. Een aantal jaar geleden bleek dat Nederland de meeste telefoontaps toepaste van de westerse wereld. Sinsdien is het aantal taps alleen nog maar toegenomen. Ook wordt er in Nederland relatief veel data in de vorm van datasets ondervangen en opgeslagen voor verdere verwerking. Gelukkig is een groot deel van de cryptografen, (wetenschaps)filosofen, programmeurs en digitale beveiligings experts het daar niet mee eens, zo kan de vrijheid van de pers ernstig gehinderd worden, oppositie gehinderd worden, burgers onderdrukt worden etc. Om die reden zijn er relatief veel technische mogelijkheden om je eigen veiligheid te verbeteren. Hieronder ga ik er meerdere toelichten. Om te beginnen ga ik het in volgende artikelen, brochures hebben over encrypted mail, tijdelijke mail, anoniem het internet op en als laatste de totaaloplossing om niet gevonden te worden.

Eerst een overzichtje van de onderwerpen:

uitleg over de termen

VPN (wat is het, de voordelen en de beperkingen, waar kan ik het krijgen)

Webbrowser aanpassen

mailservers (gratis mailservers die anoniem zijn en niet loggen)

encryptie (waarom een mailclient verstandiger is dan online mail)

anoniem het internet op (TOR en Tails)

Handige sites.

Uitleg over de termen.

Om er voor te zorgen dat deze informatie booklet begrijpelijk is voor iedereen, zal ik een zeer beknopte “crash-course” moeten geven over de termen en begrippen, die gangbaar zijn in de computer/netwerkwereld.

ISP

Dit staat voor Internet Service Provider, het bedrijf dat waar je je internet ‘afneemt’[i]

IP

De term IP, dit staat voor Internet Protocol. Feitelijk is dit nummer niets meer als het ‘adres’ van je (netwerk/internet) aansluiting. Aan de hand van databases is het mogelijk om de geolocatie van het netwerk te bepalen. Voor burgers geldt dat we via de openbare bronnen de locatie kunnen bepalen tot op stads niveau. Je precieze locaties is uiteraard bij je ISP en zij moeten deze delen met politie, justitie of een van de veiligheidsdiensten, zodra zij daar een rechterlijk bevel toe krijgen.[ii]

NODES

Nodes zijn de verbindingspunten van een netwerk (jouw computer-server waar de bezochte website op staat).

Open-source

Dit betekend dat de broncode van een prodramma openbaar is, iedereen mag en kan deze inzien. Het grootste voordeel hiervan is, dat beveiligingslekken snel te verhelpen zijn. Het merendeel van de mensen die helpen met de continue ontwikkeling van de Linux kernel zijn programmeurs, ontwikkelaars en hobbymatige ontwikkelaars. Nieuwe code wordt vaak geverifieerd en getest, alvorens ze als patch/update worden uitgebracht. Iedereen kan en mag meedoen in het testprogramma. Alleen kan dit ervoor zorgen dat je systeem instabiel wordt. Voor normale gebruikers geldt dat de stable release het beste werkt.
Een ander belangrijk punt is, dat open source software gratis is, hiermee sluit het direct mooi aan bij de anti-kapitalistische idealen van veel politieke activisten. Ook biedt open source de mogelijkheid om vrijelijk de software aan te passen, waardoor de autonomie van de gebruiker ook nog wordt versterkt. Misschien is het grootste voordeel wel dat er veel meer Windows gebruikers zijn dan open source besturings systemen, waardoor het lucratiever is om Windows aan te vallen, dan Linux distributies.[iii]

OS

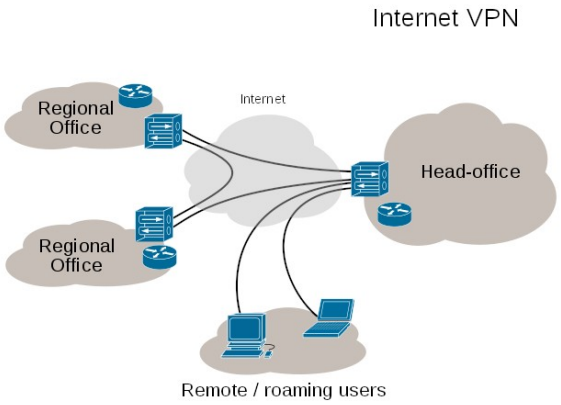
Binnen de wereld van computers wordt vaak gesproken over een OS. Hier wordt je zogenaamde Operating System mee bedoelt. Een Operating system bepaald dat je programma's kan draaien (van spelletjes tot tekstverwerkers etc.) bekende voorbeelden van een OS zijn Apple OS, Windows en op Unix gebasseerde systemen, bekende op UNIX gebaseerde systemen zijn Apple OS en freeBSD, de laatste is een gratis OS, voornamelijk gebruikt in serverparken. Hoewel het technisch geen OS is, bevatten Sony laptops (Sony Vaio) een zogenaamde rootkit. Dit is een klein programma, die bij Sony Vaio laptops voorkomt dat je een ander OS kunt installeren. Met behulp van Darik's Boot and Nuke (DBAN), dit programma draait vanaf cd, herschrijf je echter gemakkelijk elke sector van een hard drive, inclusief een eventuele rootkit, dit programma is alleen handig wanneer je je oude computer wegdoet, om alle informatie van de hard drive(s) te wissen.
Linux is een meer desktop georiënteerde afgeleide van UNIX.
Bekende Linux distributies zijn, Debian, Fedora, Ubuntu, Arch Linux, Damn Small Linux (DSL) en Mint. Voor mensen die nieuw zijn met computers, of er niet zo heel erg in geïnteresseerd zijn, zijn Ubuntu en Mint erg goed, ze bieden het gebruikersgemak van Windows, met de veiligheid van Linux. Daarnaast zijn deze distributies afgeleiden van Debian. Debian is minder gemakkelijkin het gebruik, voornamelijk omdat je relatief vaak via een command line interface werkt, ipv een grafische interface zoals bijvoorbeeld bij Apple, Windows, Ubuntu en Mint. Debian daarentegen is weer extreem aanpasbaar. De grootste 'tegenhanger' van Debian en de daar op gebaseerde systemen is Fedora. Fedora is de gratis doorontwikkeling van het niet gratis Red Hat Enterprise Linux. Red Hat is een distributie, bedoelt voor de zakelijke markt.

Email-clients

Een email-client (of Mail User Agent, MUA) is niets meer (of minder) dan een digitale brievenbus, die van verschillende adressen (mailservers) de post op kan halen. Stel jij woon aan de Dorpsstraat in Waddixveen, je partner woont aan de Marktstraat in Groningen en je werk zit aan de Wilhelminalaan in Klazinaveen. Op alle adressen krijg jij post. Het liefst heb je dan dat er een service is die al je post, gesorteerd op adres op 1 centrale plaats legt. Feitelijk doet een email-client dit, het geeft je de mogelijkheid om je email te beheren. Een andere benaming voor email-client is dan ook email handler. Er zijn meerdere email-clients , de twee bekendste zijn outlook (Windows propriatairy) en het open-source Thunderbird, van Mozilla

Wat is VPN?

VPN staat voor Virtual Protected Network, wat zoveel wilt zeggen, dat je via een openbaar netwerk (internet) eerst contact maakt met een privé netwerk (server) en daarna pas de server van je search-engine (Google, duckduckgo etc.) zie de afbeelding.
De verbinding tussen jou internet aansluiting en de VPN server is ‘getunneld’, dit betekend dat je internet-provider of de overheid/veiligheidsdiensten, niet mee kunnen kijken met wat jij aan het doen bent. Je provider ziet als enige dat je via een VPN server werkt, zij zien zowel jouw locatie (via je IP-adres) als de locatie van de vpn server (via hun IP-adres). Het is goed om te weten dat binnen Europa ALLE providers VERPLICHT zijn om al jouw contacten met andere servers te loggen (bewaren), voor maximaal 6 maanden, waarna ze de gegevens moeten vernietigen.



By Ludovic.ferre (talk · contribs) - Own work,CCBY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=10101288

Het behoeft weinig uitleg, dat je via een VPN server veel minder kwetsbaar bent om in de gaten gehouden te worden, niet alleen ziet niemand welke informatie jij bekijkt, ook je dataset (het totale pakket aan internet verkeer en metadata),vanaf je computer, wordt gereduceerd tot slechts 1 IP-adres, die verschillende momenten in de tijd wordt bezocht. Kortom je digitale voetafdruk is zeer beperkt. Nu komt de grote maar, veel VPN-servers brengen kosten in rekening. Het merendeel van de gratis VPN aanbieders, loggen je verkeer en verkopen de datasets door zowel aan overheden/overheidsinstanties, als aan commerciële ‘partners’. Oppassen dus. Nu hebben wij het geluk dat er ook meerdere ‘hacktivist’ anarchisten zijn, die niet loggende, gratis VPN aanbieden. Vaak zijn deze gebaseerd op zogenaamde ‘open-source’ software. De bekendste is openVPN, een afgeleide van de closed source CISCO free vpn, maar dan onderhouden door een grote community aan (hobby) programmeurs.

Welke VPN services zijn er?

Zoals ik al eerder zei, zijn er zowel gratis als betaalde VPN services. De meeste gratis varianten, leggen beperkingen op, vaak word je beperkt in de hoeveelheid data, de snelheid en ze loggen ook vaak. Betaalde VPN services, loggen vaak niet, beperken je minder qua hoeveelheid data en de snelheid is vaak hoger. Op internet zijn er allerlei VPN tests te vinden, toch lopen bij veel test belangrijke informatie ernstig uiteen. Volgens de ene site loggen ze geen van alle, terwijl een ander juist waarschuwd dat er een aantal dus wel loggen.

Zelf gebruik ik momenteel een betaalde VPN (Mullvad), omdat je die helemaal kan intergreren in je systeem. Eventueel kun je ook de app gebruiken, maar die maakt gebruik van een nog niet uitontwikkeld protocol, voor de beste anonimiteit heb ik de OpenVPN instellingen gebruikt.Een makkelijke en goede gratis VPN is die van Riseup.Makkelijk is dat je die niet van de grond af hoeft in te stellen, deze is beschikbaar (inclusief installatiehandleiding) voor Android, Apple (zowel mobiel als pc), Linux en Windows. Voor al deze systemen geldt, dat je het alleen maar hoeft te installeren en in je netwerk instellingen aangeven dat je systeem zelf de internet configuratie moet toepassen. Start de VPN (bij Linux de starter automatich laten starten bij iedere boot, windows doet dit automatisch) en je hebt VPN. Al het internet verkeer, vanaf het apparaat waar de riseup vpn op is geïnstalleerd gaat vanaf nu via een van de Riseup VPN servers), Ook bieden de kameraden van

autistici een gratis niet loggende VPN (uiteraard moeten zowel de autistici als de Rise up VPN onderhouden worden, een maandelijkse of jaarlijkse donatie wordt dan ook gewaardeerd)

Pas je webbrowser aan!

Om het in de gaten houden van, voornamelijk bedrijven, te beperken, bieden de meeste webbrowsers, verschillende uitbreidingen. Daarnaast bied Opera als enige een eigen gratis VPN service, of deze wel of niet logt is mij onbekend. Iedere browser gebruikt een andere benaming voor deze uitbreidingen, zo kunnen ze extensies heten, plug-ins of add-ons. Belangrijke uitbreidingen zijn NoScript, Adblocker en Trackingcookies blokkers. Tegenwoordig kan je de laatstee in de uitbreiding Pricay Badger krijgen voor Firefox van Mozilla, welke de andere browsers hebben zal je zelf moeten uitzoeken. Chrome is open-source en gebruikt nagenoeg dezelfde uitbreidingen als Firefox van Mozilla. Er is een uitbreiding, voor alle browsers beschikbaar,
die je connectie met de server zal proberen te beschermen, deze heet HTTPS EVERYWHERE.
Wel geldt dat je af en toe moet kijken of je uitbreidingen wel up-to-date zijn. Wat veel mensen zich niet realiseren, is dat veel scripts, zoals JAVA (de bekende internet spelletjes, zijn vaak in JAVA geschreven, ook veel webvideo's, geanimeerde knoppen etc.) een wezenlijk veiligheidsrisico met zich mee kunnen dragen. In de JAVA code kunnen minder leuke stukjes code verstoptzitten, waaronder worm virussen, randsomware, keyloggers etc. Gelukkig zijn er ook add-ons die dit blokkeren, een heel erg bekende is bijv. noscript. Soms zit er een scriptblocker in een adblocker verweven, zoals bij µblock. De meeste add-ons leren en updaten automatisch, waardoor je relatief weinig kans hebt op ernstige beveiligingslekken. Ook nu geldt echter weer dat de open-source platformen (Google Chrome en Mozilla Firefox), eerder een update hebben dan de closed-source browsers van Apple (Safari) en Microsoft/Windows (Explorer/Edge).
Verder zou ik ook altijd een losse wachtwoordmanager installeren, deze omzeilt de ingebouwde wachtwoordmanager van je browser, omdat die vaak minder veilig zijn een bekende en als zeer goed bekend staande is keepass

voordelen van een email-client, ten opzichte van webmail

Een grote plus van een email-client als Mozilla Thunderbird is, dat het je de mogelijkheid geeft om berichtfilters te gebruiken, die de binnenkomende mails, automatisch naar een aangemaakte map kunnen plaatsen. Dit zorgt er voor dat je inbox overzichtelijk blijft. Daarnaast zullen ze naadloos samenwerken met encryptie volgens de PGP (Pretty Good Privacy) standaard. Bij Mozilla Thunderbird, moet je dan wel eerst de add on Enigmail installeren. Overigens kan de mail-client van Microsoft, Outlook, ook overweg met de openpgp standaard, alleen moet je dan wel, net als in Thunderbird eerst een add-on installeren. Bij Outlook kun je kiezen uit gpg4o, gpg4win en p≡p.

Zelf maak ik gebruik van 3 emailadressen, bij drie verschillende mail aanbieders 1 is anoniem en puur voor acties en de VBWF(Vrije Bond West-Friesland). Dat adres eindigt op riseup.net en de afzender heet anticrust. Op dat adres wens ik nooit mijn echte naam te lezen, zolang emails niet encrypted zijn.
Mijn gmail, noem ik vaak mijn spamvanger, deze gebruik ik uitsluitend om in te schrijven bij webwinkels en dergelijke.
Voor overheidsinstanties en andere officiële zooi, gebruik ik een email met mijn volledige naam(at)mailserver.

Persoonlijk raad ik mensen altijd aan meerdere email adressen aan te maken, waarvan 1 compleet anoniem, Riseup.net biedt dit ook aan, uiteraard zijn er meerdere radicale (mail)servers, de mensen van Riseup hebben daar een lijst van, op www.riseup.net vindt je alle info over hun webmail en een how to Riseupvpn installeren (voor alle platformen, inclusief Android) .

Encryptie

Het grootste voordeel van een email-client is toch wel de mogelijkheid om via het POP3 protocol, mails worden dan van de server gehaald en lokaal opgeslagen. Dit heeft als voordeel dat wanneer de servers van je email provider in beslag worden genomen, jouw (gevoelige) mail communicatie niet meer op de server staat. Voorwaarde is wel dat je je harde schijf encrypt hebt (mocht jouw computer ooit door de politie worden meegenomen, kunnen ze iig niet zo veel met je harde schijf. Het compleet encrypten van schijven is het veiligst, maar het betekend ook dat je schijf wel leeg moet zijn, alles wat er opstaat wordt door de encryptie onherstelbaar vernietigd. Uiteraard kan je ook aparte bestanden via het truecrypt protocol versleutelen, moet jer echter wel voor zorgen dat de log en encyptiemappen van je encryptionprogramma op een vooraf encrypted schijf staan. Veruit de meeste Linux distributies, geven je de mogelijkheid om iig de schijf waar het OS op komt, te encrypten. Hoe dit met Windows zit, weet ik niet, daar ik al ruim 10 jaar alleen Linux gebruik.

Internet en anonimiteit, TOR

Regelmatig wordt er in de media gesuggereerd dat mensen op Social media veel durven te zeggen, omdat ze anoniem zijn. Dit is dus niet zo. Via de servers van Facebook (die staan zowel in Ierland als in Amsterdam), kan de overheid altijd de logfiles opvragen van gebruikers (feitrelijk geld dit voor alle servers binnen de EU en de verschillende samenwerkingspartners op het gebied van de IT/ ICT). Deze logfiles bevatten altijd het IP adres, ook bevatten ze vaak informatie over eventueel gebruikte nodes. Om dit minder traceerbaar te maken, kan je meer nodes gebruiken. Zie hier direct de techniek achter TOR. TOR staat voor The Onion Network (het uien netwerk). Deze naam slaat op de wijze waarop de TOR browser werkt. Doordat je verbinding via verschillende nodes gaat, wordt het steeds moeilijker om bij de bron te komen. Iedere node is als het ware een laag van een ui. De programmeurs achter het TORproject raden het gebruik van TOR over VPN af, omdat niet alle VPN protocollen om kunnen gaan met TOR. Sinds enige tijd heeft TOR echter de optie om een bridge (brug) te gebruiken. Deze brug maakt het mogelijk voor mensen in landen, waar strenge internet censuur heerst (en een autoritair regime aan de macht staat) probleemloos het internet op kunnen, dit gebeurt door de gebruikte communicatie poort te verbergen. Voor mensen in ‘open landen’ (EU, VS, Japan, Auid Korea etc) heeft het bridgen geen meerwaarde. De TOR browser biedt overigens ook de mogelijkheid tot heel het internet (alles wat je via Google kan vinden is slechts 20% van het internet, de overige 80% staat bekend als het darkweb/darknet. Dat is het minder leuke deel van het internet, vol met wapen-/drugs-/vrouwen- en kinderhandel. Ook kan je daar de meer radicale fora van neo-nazi’s en fascisten vinden, kortom niet zo gezellig daar. Omdat de afgelopen jaren steeds vaker mensen drugs wilde bestellen via het darkweb, ontwikkelde iemand een TOR plug-in. Deze laat je, via de Mozilla Firefox webbrowser, vanaf het reguliere internet, onafgeschermd direct contact maken met servers van het darkweb. Dit heeft uitendelijk veel Amerikaanse studenten hun vrijheid gekost, immers kon iedereen met verstand van internet meekijken met hun bestellingen aan drugs, zo ook de politie. Het behoeft verder geen uitleg dat die bewuste plug-in niet erg veel te bieden heeft. De TOR browser is er voor ieder platform, ook voor de mobiele platforms. Wil je meer weten over TOR, klik dan op de link hier.

Ondanks de extra anonimiteit, blijft TOR 1 nadeel hebben en dat is dat je beter geen scripts kan draaien als Java, omdat die alsnog je locatie kunnen vrijgeven.

TAILS

Tails (The Amnesic Incognito Live System) is een zogeheten Live-systeem, wat betekend dat je de standaard Tails, op elke computer kan draaien met een usb poort of een dvd drive. Het op Debian gebaseerde systeem draait als een live systeem, wat wil zeggen dat het tijdelijk draait op een computer. Tails laat geen sporen achter op de pc en alle verbindingen gaan standaard via het TORnetwerk. Voor riskante/gevoelige acties is Tails best practice, omdat je letterlijk vanaf vrijwel iedere computer met een internetverbinding anoniem het internet op kan, de bewuste computer wordt bij het afsluiten compleet gewist van alle data van Tails. Omdat Tails op een usb stick past, kan je altijd en overal op iedere pc, geheel onbekend het internet op. Bezoek de site van Tails hier, wel is het verstandig om zodra je TAILS hebt, je er bekend mee te maken, vooral mensen die in het dagelijks leven Windows gebruiken, raad ik dit aan. Overigens is het ook voor de Linux gebruikers best practice om regelmatig met TAILS te werken.

“conclusie”

Voor mensen die privacy en digitale veiligheid belangrijk vinden, zoals (politieke) activisten, journalisten en klokkenluiders geldt vaak dat ze absoluut wegblijven van alle Microsoft, Apple en Sony (VAIO) producten. Omdat Android bebaseerd is op Linux, zijn er mogelijkheden om het systeem te beschermen tegen haar boosaardige ontwikkelaar Google, daarnaast is iedere Android versie via verschillende instelling bijna geheel los te koppelen van Google, Alleen de Google play store blijft nodig, omdat Google voortaan de systeemupdates via dat platform wilt gaan aanbieden. Hoewel veel open-source sogtware en systemen veel veiliger zijn, behoeven ze meer aandacht, zijn ze minder gebruiksvriendelijk, maar heb je indien nodig, wel complete controle over je systeem.

Wil je wel grotendeels (99%) dezelfde veiligheid, maar minder vertrouwen op je eigen know-how, dan zijn er distributies zoals Ubuntu en Mint, welke als doelstelling hebben om een zeer gebruiksvriendelijk Linux based systeem te maken. Voor de echte Linux liefhebbers zijn er ook distrro’s die heel basic zijn, een voorbeeld hiervan is Arch linux, deze distro is compleet kaal, heeft alleen de werkende Linux kernel en moet nog geheel worden opgebouwd. Ook bij Debian is dit mogelijk, maar voor nieuwe gebruikers of hobbyisten die geen ‘commandline’ almanak naast zich willen hebben liggen, zijn deze te basic. Omdat Linux systemen compleet aanpasbaar zijn, kan je zelf een grafische interface kiezen, waardoor je een Windows-achtige interface kan kiezen (KDE) een complete tegenhanger (GNOME), een bijzonder lichte, afgeleid van KDE (XFCE) of een even lichte afgeleide van GNOME (LXDE). Er zijn nog andere ‘smaakjes’, meestal zijn dat dan meestal weer,afgeleide van GNOME, toegespitst op een bepaalde functionaliteit, zoals een mediaserver.

Mensen die liever ook in het dagelijkse leven meer veiligheid op internet willen, moeten beginnen bij hun browser. Persoonlijk kies ik voor Mozilla Firefox, mede omdat het open-source is, ook omdat ik die al jaren gebruik.
Wil je gemakkelijk meerdere mailaccounts beheren, neem dan een email-client. Voor windows is er al een standaard, bij Linux heeft iedere distro zijn eigen, maar alle distro’s leveren thunderbird via hun software pakketten.
Als je een apart mailaccount aanmaakt voor actiedoeleinden, is het belangrijk om dat mailaccount te beveiligen. Wel moeten mensen dan onderling hun publieke sleutels ruilen, maar dat hoeft geen probleem te zijn.

Zodra je internet gebruik een eventueel risico kan opleveren, bijv. je doet onderzoek en wilt geen neonazi’s aan je deur, gebruik een VPN (minimaal), TOR of TAILS

Ga je op vakantie, maar je zou nog wat uitzoeken? Geen nood, neem je usb stik met Tails mee!

Over de verschillende onderdelen, die ik nu kort heb beschreven, zal ik in de komende maanden meer uitgebreid over gaan schrijven. Ook zal ik tzt, ook nog iets schrijven over verschillende messenger apps voor android.

Met anonieme groet,
Anticrust

HANDIGE links

www.gratissoftwaresite.nl
https://ubuntu.com
www.debian.org
www.torproject.org
https://tails.boum.org
https://riseup.net/en
https://riseup.net/en/security/resources/radical-servers

i https://www.lifewire.com/internet-service-provider-isp-2625924
ii http://www.wetboek-online.nl/wet/Wetboek%20van%20Strafvordering.html#830
iii http://techgenix.com/Open_Source_Secure/