Etienne van Rattingen – natuurfilosoof

15 minuten anonimiteit

Om er voor te zorgen dat data, verzonden via internet, veilig is, is geen eenvoudige zaak. Niets is privé op internet en iedereen kan aan het snoepen zijn om meer te weten over u, uw handel of uw bedrijvigheid. Google, Windows, Facebook, Instagram, LinkedIn, Amazone zijn allemaal spionage-tools om u allerlei gegevens te ontfutselen. Ik weet dat u mij niet gelooft. Voor mij geen probleem. Er zijn mensen die weten dat het wel zo is. Voor hen schrijf ik dit neer. De ongelovige mag dit artikeltje met een 'gerust' hart negeren. Tenslotte is het UW privéleven dat op straat komt te liggen, niet het mijne! Van Google en Facebook is bekend, dat ze miljoenen per jaar krijgen van de CIA om gegevens met hen te delen. Facebook is daarbij persoonlijk bezit van grootbank, oplichter, dief en fraudeur Goldman Sachs, ze delen hetzelfde adres in London city. Waarom is een bank feitelijke eigenaar van een 'sociale' netwerksite? Roept dat geen vragen op?

Er zwerven vele verschillende encryption tools rond. Het is zaak om bijvoorbeeld BitLocker van Microsoft niet te gebruiken omdat er wel een achterdeur voor NSA, CIA en andere inlichtingendiensten waar ze mee samenwerken zal zitten, zoals in al hun Operating Systemen. Programma's, waarvan de programmeercode niet vrij te verkrijgen is, blijken veel stank te verspreiden. Geloof me, dat wil je niet op je computer hebben.

Het maakt niet uit wat voor O.S. je draait op je box. Alles kan zeker veilig gehouden worden tijdens uitwisseling van data. Daar niet iedereen een computervirtuoos is, kunnen een paar kleine installaties en veranderingen van mentaliteit al voor heel wat meer privacy zorgen.

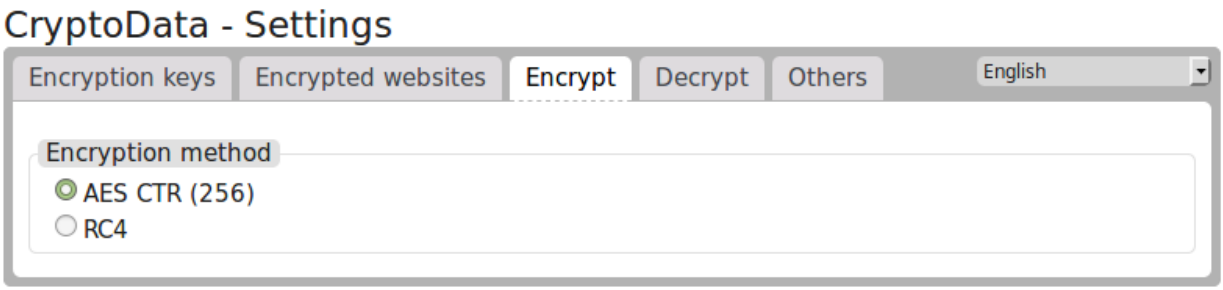
Wat je wel moet weten is, dat Windows 10 niet veilig kan worden gemaakt. (zie mijn artikel over Windows 10 op de site) Verder mag je geen gebruik maken van Microsoft Internet Explorer of Chrome. Installeer Firefox om te communiceren op veilige manier. Zorg ervoor dat privé surfen is aangevinkt zodat u ook niet gevolgd kan worden via 'tracking' cookies. U moet weten dat alles van Microsoft in feite al gehackt is en nooit in aanmerking zou mogen komen om deze shit op argeloze burgers hun PC te installeren om hen ongestoord en met behulp van overheden te kunnen bespioneren. Overheden respecteren uw PRIVACY helemaal niet. Indien ze dat zouden doen was alle brol van Microsoft over heel de wereld verboden.

Ik heb geen probleem om de waarheid neer te schrijven. Mijn vele contacten wereldwijd maken alles mogelijk. Dan blijkt pas in wat voor een droomwereld meeste mensen leven. Ze beseffen niet eens dat ze in een leugen leven. Mijn specialiteit heeft het mogelijk gemaakt dat het ook ECHT veilig kan, zelfs voor een leek.

Met alles wat ik u ga 'leren' geef ik wel de raad om sleutels en paswoorden nooit via mail te verstuuren. Gebruik een 'dedicated' computer voor veilige communicatie. Dat is een computer die u voor NIETS anders gebruikt. Herinstalleer deze regelmatig.

Omdat weinig mensen beseffen hoe gevaarlijk internet is

Voor mensen die zo nodig willen chatten, gebruik CryptoCat. Er is ook een extensie voor deze applicatie in Firefox.



Files uitwisselen

Als je op een veilige manier en ook anoniem mail wil versturen dan kun je gebruik maken van betaalde en onbetaalde services. https://spideroak.com/ en https://www.hushmail.com/ zijn zeer goede oplossingen. Toch prefereer ik gebruik te maken van mogelijkheden door mijn zielsverwanten geschapen in Duitsland. https://anonbox.net/ is mogelijk gemaakt door https://www.ccc.de/en/ maar ik geef de waarschuwing om altijd gebruik te maken van alle mailservices via TOR.

Vele leuke web proxies zijn door de jaren verdwenen naar Deep Web omdat overheden op hen joegen. Deep Web is een wereld op zich. Wordt door allerlei dip sticks van journalisten verkocht als de ONDERWERELD van internet, terwijl het gewoon een ontsnapping is aan de BIG BROTHER maatschappij. Deze schrijvende EIKELS moesten eens weten hoeveel ECHTE journalisten gebruik maken van de Deep Web mogelijkheden om anoniem te kunnen blijven en de waarheid boven tafel te krijgen over al degenen in wiens kont wordt gekropen in uw artificiële wereld. Natuurlijk zijn er ook websites waar drugs, wapens en huurmoordenaars worden aangeboden. Toch deze onzin beslaat waarschijnlijk nog niet eens 1% van alles wat er in het Deep Web beweegt en aanwezig is. Deep Web bestaat omdat BIG BROTHER bestaat. Omdat overheden ALLES willen kunnen controleren. Wel, dikke pech! Deep Web kan wel gemonitord worden maar alle verkeer blijft ten alle tijde anoniem. Ze zullen nooit kunnen uitmaken wie er achter welke communicatie zit. En, als deze communicatie ook nog een keer geëncrypteerd is, zullen ze zelfs de boodschap niet kunnen lezen, zoveel is zeker.

Geheime nota's

https://privnote.com/ is één van de beste encryptietools om korte memo's te versturen die zichzelf vernietigen nadat ze zijn gelezen. Het is praktisch om een paswoord te verzenden zodat bijvoorbeeld mails niet eens verstuurd moeten worden. Het paswoord is bijvoorbeeld voor een gedeelde mailaccount zodat uw mede opponent niet verstuurde mails kan lezen en daarna wissen.

ZeroBin (http://sebsauvage.net/paste/) gebruikt hetzelfde principe maar hierin kunt u exact aangeven wanneer de boodschap MOET worden gewist, ongeacht of deze is gelezen. Ook hiervoor hoort een connectie via TOR te worden gemaakt om echt veilig te zijn.

Alternatieven voor Skype

Sinds Microsoft eigenaar is van Skype, is de encryptie niet langer veilig. Vele inlichtingendiensten in de wereld, allemaal holmaatjes van NSA en CIA, kunnen nu doodgemoedereerd inbreken in elke conversatie en meeluisteren. Sinds 2005 zijn er aangepaste Skype versies in omloop waarin politiediensten ook kunnen meeluisteren. Vele regeringen VERBIEDEN gebruik van Skype aan hun ambtenaren en medewerkers. Het BIG BROTHER gedrag van Microsoft heeft al aan ettelijke journalisten het leven gekost. Daarom zijn we ook naar ander manieren gaan kijken om VEILIG te kunnen communiceren.

Als je wilt telefoneren via internet zijn er twee veilige oplossingen. https://jitsi.org/ is de open source oplossing voor SKYPE. Het werd aanbevolen door Jacob Appelbaum, een hacker en medeontwikkelaar van TOR. Ook was hij woordvoerder voor WikiLeaks en dus serieus op de hoogte over hetgeen veilig is om als open source te gebruiken.

Ook Mumble is een fantastische oplossing om geëncrypteerde boodschappen te versturen. Eigenlijk wordt het gebruikt door videogamers maar alle tekstboodschappen zijn versleuteld. Tijdens de Arabische Lente maakten we hiervan gebruik om de waarheid over deze ‘opstand’ in de richting van Noord Afrika te sturen. Daarom werd dit SOROS hersenspinseltje ook een groot fiasco. Alleen zonde dat Libië is gevallen. De bedoeling van de Arabische Lente was in feite alle noord Afrikaanse landen zodanig te destabiliseren dat ganse stromen met noord Afrikanen op de been zouden komen om via Spanje, Italië en Griekenland Europa te overspoelen.

Dan zouden we niet spreken over ettelijke miljoenen vluchtelingen maar eerder van ettelijke tientallen miljoenen. Nu gebruikt SOROS zijn Ngo’s dieper in Afrika om daar vluchtelingenstromen vanuit Soedan en dergelijke landen op gang te brengen. Wij als hackers kunnen deze mensen niet bereiken om hen te waarschuwen voor deze Ngo’s omdat ze geen internetaansluiting hebben en waarschijnlijk te arm zijn om een computer te hebben.

Indien EU politici een paar ballen aan hun lijf hebben, sturen ze de rekening voor alle gemaakte kosten en verdere onderhoudskosten voor ‘vluchtelingen’ naar SOROS. Op deze manier wordt de Europese BELASTINGBETALER volledig ontzien. Nu moeten we voor alle kosten opdraaien.

Computer Security

Verzorgen van digitale veiligheid is een specialisatie in de IT wereld. Indien u geen security expert bent moet u er rekening mee houden dat u altijd gemonitord wordt. Internetproviders houden alles bij. Niet dat ze dat willen maar omdat de wet hen dit verplicht. Voor gsm-gebruik is dat exact hetzelfde. Alle nummers die u belt of door wie u wordt gebeld, worden allemaal bewaard. De staat VERPLICHT providers u te bespioneren. **Een overheid heeft het schijt aan uw privacy!**

Omdat weinig mensen beseffen hoe gevaarlijk internet is