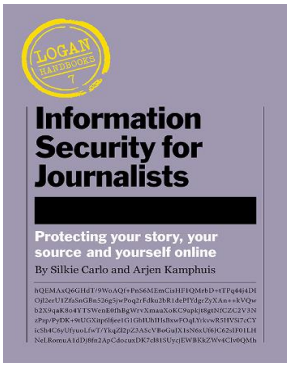
Informatiebeveiliging voor (o.a.) journalisten



Het online beschermen van jezelf, je verhaal en je bron

door Silkie Carlo en Arjen Kamphuis

Nederlandse vertaling door Helma de Boer
versie 1.1 – januari 2018

Dankwoord

Allereerst wil ik Arjen Kamphuis mijn grote dank betuigen voor zijn geduld en genereuze uitleg.

Veel dank gaat uit naar Gavin MacFadyen († 2016) en de CIJ die ons deze opdracht en de verantwoording hebben gegeven om een boek te schrijven dat het doel heeft om journalisten en hun bronnen te beschermen en tot het uitdragen van informatiebeveiliging in het algemeen.

We bedanken alle klokkenluiders en hacktivisten en niemand minder dan Edward Snowden, voor het openbaar maken van de informatie waar we nu van profiteren en waarmee we onszelf, onze bronnen en de vrije pers kunnen beschermen

In solidariteit met en dankbaarheid naar de journalisten die van plan zijn deze handleiding te gebruiken.

Silkie Carlo – London 2016

Dank aan de helden van de Free Software Foundation die de problemen die we nu hebben, dertig jaar geleden al voorzagen en ermee aan de slag gingen, zodat we nu alternatieven hebben.

Dank aan de ontwikkelaars en hackers die hun werk gratis delen met de mensheid.

Dank aan Gavin, Juliet en Minal bij CIJ voor al hun goede werk in de ondersteuning van journalisten (inclusief de ondersteuning aan ons bij het maken van dit boek).

Dank aan de klokkenluiders, voor hun dapperheid en opoffering.

En dank aan mijn coauteur Silkie Carlo, voor haar nieuwsgierigheid, drive, kalmte en het niet genoegen nemen met minder dan het beste.

Ik draag dit boek op aan mijn ouders, Ida en André Kamphuis, die mij leerden altijd achter mijn principes te blijven staan en mijn hoofd nooit te buigen voor autoriteiten die deze principes proberen kapot te maken.

Arjen Kamphuis – Berlin 2014

Dank aan Helma de Boer voor het maken van de Nederlandse vertaling van 'Information Security for Journalists'

Arjen Kamphuis – London 2017

Inleiding - Silkie

In 2014 verscheen de eerste publicatie van dit handboek, drie jaar nadat Edward Snowden de klok luidde over massasurveillance. Hij offerde voor dit onderwerp zijn vrijheid op in de hoop dat anderen die van henzelf zouden kunnen teruggrijpen en beschermen.

In de tussentijd hebben we ontdekt dat in de jaren tussen 2011-2014 op zijn minst 100 journalisten en meer dan 240 bronnen in het Verenigd Koninkrijk zijn bespioneerd door de politie (IOCCO, 2015). De krant 'The Guardian' kreeg bezoek van spionnen die systematisch harddrives vernietigden waarop brondocumenten stonden. David Miranda werd vastgehouden en ondervraagd op basis van de Terrorism Act; en de laptop van een BBC Newsnight journalist is ingenomen op basis van dezelfde wet.

De reactie van de overheid op de onthullingen en verschillende juridische uitdagingen, was de Investigatory Powers Bill. Wetgeving in het Verenigd Koninkrijk die de overheid buitengewoon veel macht geeft tot massasurveillance inclusief hacking, het opnemen van ieders persoonlijk gebruik van internet, het bouwen van databases met informatie op een enorme schaal en de mogelijkheden om doelwitten te onderscheppen en te hacken zonder dat daar een redelijke verdenking van het plegen van een misdaad voor hoeft te zijn. Bescherming van journalisten zoals die in de eerdere wetgeving bestond, is vreemd genoeg afwezig in deze wet. Geen enkele informatie is off-limit in de nieuwe surveillancestaat.

De draconische massasurveillance die op dit moment wordt uitgevoerd, vindt plaats terwijl we nog maar aan het begin van het verhaal van democratie in het digitale tijdperk staan. De gemeenschappelijke reactie hierop zal aantonen hoe goed we in staat zijn om vrijheid van meningsuiting en het recht op een privéleven in de toekomst te beschermen.

Wanneer journalistiek betekent dat je iets schrijft wat een ander niet geschreven wil hebben – en voor onderzoeksjournalistiek is dat meestal het geval – dan moet je aannemen dat je tegen de tijd dat je je beste werk schrijft, je een tegenstander hebt tegen wie je jezelf, je verhaal en je bronnen moet beschermen. Vanaf het moment dat Edward Snowden als klokkenluider naar buiten trad op 5 juni 2013, vond ik het belangrijk om mezelf te verdiepen in de informatiebeveiligingsmethodes (ook: infosec) die vrijheid van meningsuiting en persvrijheid beschermen. Daarmee bedoel ik simpele methodes die, zonder overdrijving, essentieel zijn om deze kritische mensenrechten te bewaren en verbeteren. Ik ben het levende voorbeeld van het feit dat iedere vastberaden onderzoeksjournalist die het geduld heeft om te leren, al snel een gevorderde gebruiker van de infosec-methodes wordt.

Dit handboek is in zo duidelijk mogelijke termen geschreven, met begrijpelijk instructies zonder in te leveren op kennis, onderricht of veiligheid. Zo heb je een snelweg in het leerproces. De beste manier om te leren is door te doen, dus ik raad je aan dit handboek te gebruiken vanaf het moment dat je hardware wilt aanschaffen.

Ten slotte nog belangrijk; ik hoop dat dit handboek een grote groep onderzoeksjournalisten en hun bronnen in staat stelt om hun privacy te beschermen. Maar als dit handboek maar één slachtoffer van onrechtvaardigheid of één getuige van criminele activiteiten helpt om zijn verhaal te vertellen, als het ervoor zorgt dat één persoon veilig met de wereld kan communiceren en zijn stem wordt gehoord, dan heeft dit handboek zijn doel uitstekend gediend.

Silkie Carlo, Londen 2016

Inleiding- Arjen

Sinds de onthulling van Snowden blijken de meest extreme, paranoïde angsten van privacy-activisten en informatiebeveiligings-experts bijna aaibare, kleine problemen te zijn vergeleken met de realiteit van de industrialisatie van spionage over onze hele planeet. Iedere journalist die de ontwikkelingen over de laatste onthullingen heeft gevolgd, en het verlangen heeft om zijn bronnen en verhalen te beschermen tegen overheden en grote bedrijven die rondneuzen, heeft wellicht wanhoop gevoeld.

Is alles met een chip en een batterij ons aan het bespioneren? Als je de meeste apparaten bekijkt zoals die in de winkel op de plank staan, zoals laptops, tablets en smartphones, is de situatie inderdaad erg. Maar er zijn maatregelen die je kunt nemen en die steppen zijn niet duur en je hebt er ook geen PhD computerwetenschappen voor nodig. Het gebruik van een computersysteem dat vrijwel alle geavanceerde aanvallen door de meest geavanceerde nationale overheden kan weerstaan, ligt binnen ieders bereik. Tenminste, iedereen die bereid is een paar dagen te besteden om gratis software te leren gebruiken en wil leren omgaan met hardware die je al in het bezit hebt of die je voor minder dan € 300,- kunt aanschaffen.

Dit handboek helpt je op weg hoe je jouw data en communicatie en dat van je bronnen kunt beschermen en leert je hoe je middelen en methodes kunt gebruiken die zichzelf in de meest extreme situaties hebben bewezen door experts wereldwijd. Afhankelijk van je huidige computervaardigheid kan dit enigszins een leerproces zijn, maar weet dat velen je zijn voorgegaan die zichzelf niet als experts beschouwden en die er desondanks in zijn geslaagd om naar tevredenheid te werken met de methodes en middelen die we in dit boek beschrijven.

Als je in de 21e eeuw een journalist bent, dan heb je deze tools nodig. Immers, William Randolph Hearst zei decennia geleden: "*Journalistiek is opschrijven wat machtige mensen en instituten niet opgeschreven willen hebben*."

Als je jezelf niet beschouwt als journalist, maar gebruik wilt maken van je recht op privacy zoals je dat wordt gegarandeerd in de UN Declaration Of Human Rights [1948] Article 12, dan is dit boek ook voor jou.

Zoals bijna iedereen die ooit iets heeft gemaakt weet, kunnen we alleen iets maken op basis van de kennis van duizend generaties voor ons. Daarom zal dit boek voor altijd gratis verkrijgbaar zijn in een serie verschillende digitale formaten, zonder enige restrictie. Als er een format ontbreekt waarin je het graag wilt hebben, laat het ons weten.

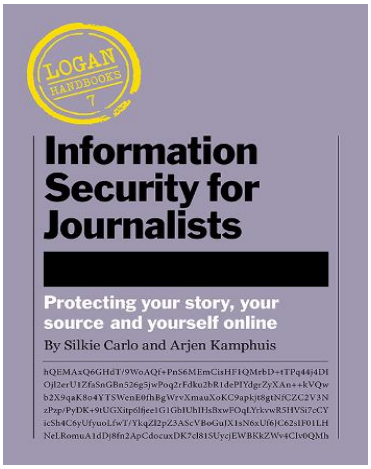
Als je waardering hebt voor dit boek, verspreid het dan zoveel mogelijk en help ons om de volgende versie beter te maken. Constructieve feedback in wat voor vorm ook, is zeer welkom. Het privacy-probleem zal zich alleen verder ontwikkelen, en dat geldt dus ook voor ons antwoord daarop. Help daarom mee door de kennis te delen en dit boek en de beschreven hulpmiddelen op wat voor manier dan ook te promoten.

Arjen Kamphuis, Berlijn 2014

Inhoudsopgave

Gratis download

Wij zijn heel blij dit handboek te kunnen aanbieden als gratis download en we willen dat graag zo houden.



Vind je het boek bruikbaar of wil je helpen om ervoor te zorgen dat het beschikbaar blijft voor degenen die zich eventuele aankoop niet kunnen permitteren? Overweeg dan om een **donatie** te doen.

Hartelijk dank namens the Centre for Investigative Journalism.

Download het boek (versie 1.1 – NL, alleen als PDF).

Hier vind je de Engelse versie van dit boek (mei 2016).

Voorwoord Gavin MacFadyen, CIJ

Dit handboek is een belangrijk praktisch hulpmiddel voor journalisten, in het bijzonder onderzoeksjournalisten. Tegenwoordig zijn journalisten zich ervan bewust dat vrijwel iedere vorm van verzonden of ontvangen elektronische communicatie wordt opgenomen, vastgelegd en onderwerp van analyse is. Omdat deze vorm van surveillance in het geheim wordt uitgevoerd, zonder enige terughoudendheid, transparantie of enige realistische vorm van verantwoording, bedreigt dit de verhalen en het professionele werk van journalisten.

De nieuwe wetgeving van de Britse overheid over surveillance, de 'Investigatory Powers Bill', markeert een stap die een onthutsend grote afstand neemt van juridische principes rondom bronbescherming, alles ten gunste van ongebreidelde spionagemogelijkheden door de overheid.

De realisatie dat tegenwoordig bijna alle digitale communicatie wordt vastgelegd, heeft tot flinke verontrusting bij journalisten geleid. Die massasurveillance brengt letterlijk risico's en gevaren voor hen en hun bronnen met zich mee. Die gevaren zijn niet alleen een probleem voor journalisten, klokkenluiders en andere bronnen; ze vormen problemen voor iedereen die te maken heeft met gevoelige informatie en voor iedereen voor wie privacy fundamenteel is. Denk bijvoorbeeld aan rechtbanken, bij het uitoefenen van justitiële beroepen en bij rechtspraak in al zijn vormen. Advocaten, accountants, artsen en hun cliënten ontberen de bescherming van cliëntvertrouwelijkheid en zijn kwetsbaar vanwege de geheime surveillance door een groeiend autoritaire en onverantwoordelijke overheid.

Na Snowdens onthullingen aan het publiek, is het duidelijk dat er ook goede maatregelen ter bescherming beschikbaar zijn. Dit handboek (The CIJ's handbook, Information Security for Journalists), beschrijft de meeste effectieve manieren om je werk privé te houden, veilig van spionage. Het legt uit hoe je veilig kunt schrijven, hoe je met beveiliging moet omgaan en hoe je veilig informatie kunt ontvangen, opslaan en verzenden waarvan een overheid of machtige corporate liever niet heeft dat je die informatie kent, hebt of deelt. Om jouw privacy en de veiligheid van je bronnen te verzekeren, helpt Information Security for Journalists je om je communicatie anoniem, niet ontcijferbaar en niet te detecteren te maken.

Als je werkt aan een onderwerp dat privé en vertrouwelijk moet blijven, is het belangrijk om zorgvuldig te overwegen welke mate van gevaar er met het werk gemoeid is. Onderwerpen als winkelonderhoud, gezondheid en veiligheid op de bouwplaats, hygiëne in restaurants en de uitbesteding van schoonmaak in ziekenhuis, zijn wellicht gebieden waarvoor de in dit boek beschreven voorzorgsmaatregelen en methodes onnodig zijn, of het werk te veel compliceren en vertragen. In die gevallen volstaat in de eerste contacten waarschijnlijk een telefoontje die ver van werk of thuis wordt gemaakt met een bron of journalist.

Mensen die verslag doen over of werken aan nationale veiligheid, defensie, verwerking van belangrijke gegevens, nucleaire zaken of mensen die op een hoog niveau werken bij de overheid of grote corporates, moeten overwegen dit handboek als een belangrijk instrument te zien voor hun eigen veiligheid.

Dit handboek gaat vooral over hoe je je computer veilig kunt gebruiken, maar desondanks hoef je geen bijzondere opleiding te hebben in computertechnologie om de instructies te kunnen gebruiken. De auteurs en andere experts die adviseerden in dit project, hebben ervoor gezorgd dat het een

praktisch en bruikbaar hulpmiddel is. De verwachting is dat er met enige regelmaat aanpassingen volgen. Ga daarom eens per jaar terug naar nvj.nl om de nieuwste versie te downloaden.

Zorg ervoor dat het downloaden van het handboek niet kan leiden tot identificatie van de computer waar jij mee werkt, niet bij je werkgever, je bron en of thuis.

Gavin MacFadyen, *(01-01-1940 - 22-10-2016)*
directeur Centre for Investigative Journalism

London, 2014

Introductie

Stel je eens voor dat je je inbox opent en je vindt er een anonieme e-mail van iemand die belangrijke informatie, gevoelige documenten met grote internationale importantie met je wil delen. Die bron en de informatie hebben beveiliging van het hoogste niveau nodig.

Wat doe je?

Dit handboek is gemaakt als instructie voor journalisten en mediaorganisaties om te leren hoe je met informatiebeveiliging in het digitale tijdperk moet omgaan, hoe je je werk, je bronnen en je communicatie op verschillende risiconiveaus kunt beschermen.

Informatiebeveiliging (ook wel infosec, 'Information security') is de verdedigingslijn tegen ongeautoriseerde toegang van je informatie. De informatie in kwestie kan een verslag zijn waar je aan werkt, alle bestanden die daarbij horen, de identiteit van je bronnen, je communicatie met hen en soms je eigen identiteit.

Je hoeft geen IT-expert te zijn om infosec toe te passen, hoewel je zeker veel leert als je ermee aan de slag gaat. Als je dit handboek gebruikt, leer je binnen een paar dagen hoe je versleutelde e-mailberichten en documenten kunt versturen vanaf je eigen uitstekend beveiligde laptop.

De bedreigingen: wie vormt een bedreiging?
De onthullingen van Snowden tonen aan dat bepaalde inlichtingendiensten van de overheid exorbitante mogelijkheden hebben om communicatie te onderscheppen en ongeautoriseerde toegang te verkrijgen tot data van vrijwel iedere pc of elektronisch communicatie-apparaat in de wereld. Dit kan een informatieveiligheidsrisico vormen voor onderzoeksjournalisten die werken aan verhalen die tegen de belangen ingaan van die overheden, hun diensten en de gecontracteerde private veiligheidsorganisaties.

Veel landen hebben niet zulke uitgebreide, verfijnde technologieën, maar alle landen hebben surveillancevaardigheden die gebruikt kunnen worden en soms ook gebruikt zijn tegen journalisten met mogelijk ernstige consequenties voor die journalisten. Ethiopië, een technologisch minder ontwikkeld land, wordt ervan verdacht aanvallen op afstand te hebben uitgevoerd op journalisten die daar in Amerikaanse kantoren werkten.

In dit tijdperk van globalisering hebben sommige transnationale organisaties grotere rijkdom en macht dan veel soevereine nationale staten. Daarmee in overeenstemming hebben deze soms ook meer capaciteiten/mogelijkheden op het gebied van veiligheid en surveillance dan overheden.

Het zijn bovendien niet alleen grote corporaties, maar ook verfijnde criminele organisaties waarvan bekend is dat ze indrukwekkende surveillancetechnologieën hebben. Sommige criminele organisaties hebben zelfs wellicht een overlap met criminele elementen in de overheid. Het leger van Mexico besteedde $350 miljoen aan surveillancemiddelen tussen 2011-2012. In diezelfde periode zijn negen journalisten in Mexico vermoord vanwege hun werk. Er wordt gerapporteerd dat het leger ondertussen technologieën heeft om tekstberichten, telefoongesprekken en e-mails te verzamelen, om op afstand audio van mobiele telefoons op te nemen en zelfs om beweging te detecteren door muren heen met radartechnologie.

Ongeautoriseerde toegang kan inhouden dat je data wordt misbruikt, onthuld, verstoord, aangepast, geïnspecteerd, opgenomen of vernietigd. Het kan jezelf en je bron in juridische of fysieke problemen brengen en de informatie kan in het hart van je verhaal worden getroffen of gecompromitteerd. In situaties waar sprake is van een hoog risiconiveau, kan infosec net zo belangrijk zijn als het dragen van een kogelvrij vest en het reizen met bodyguards. Maar omdat digitale gevaren onzichtbaar, gecompliceerd en vaak niet te detecteren zijn, kunnen ze gemakkelijk worden onderschat of over het hoofd worden gezien.

Sleepnetgevaar (dragnet)
Je zult je waarschijnlijk willen beschermen tegen zogenaamde sleepnet- of dragnet-surveillanceprogramma's van US National Security Agency (NSA) and the UK Government Communications Headquarters (GCHQ). Deze programma's verzamelen alle onlinedata en telecommunicatiedata ter wereld en kunnen deze analyseren. Waarschijnlijk is er onderzoek met terugwerkende kracht in de verzamelde gegevens mogelijk. Ook politiediensten in het Verenigd Koninkrijk hebben opgeslagen data ingezien om honderden journalistieke bronnen te identificeren (IOCCO inquiry into the use of Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act (RIPA) to identify journalistic sources, 4 februari 2015).

Infosec toepassen
Als je een effectieve journalist bent, zul je in de loop van je carrière merken dat je een paar wespen in hun nest verstoort. Daarom is het belangrijk om goede infosec toe te passen. Het moet gewoon worden om verschillende strategieën structureel te gebruiken die je gemakkelijk in je dagelijkse werk kunt inpassen. Het betekent ook dat je per geval moet bekijken welke beschermingsstrategie je moet toepassen. Die strategie verandert en vraagt meer van je als je sterkere infosec-methodes moet gebruiken als je aan gevoelige onderwerpen en/of met kwetsbare bronnen werkt.

De eerste stap om goede infosec toe te passen is daarom de bewustwording van de gevaren. De tweede stap is om je bewust te zijn van de kwetsbaarheden in je hardware en software. Het begrijpen van waarom en hoe kwaadwillende ongeautoriseerde toegang willen en krijgen, is de belangrijkste stap in het leerproces om jezelf ertegen te beschermen.

Legaliteit van de hulpmiddelen
Ondanks het feit dat de zeer uitgebreide surveillance van burgers die de wet respecteren vrijwel zeker indruist tegen de internationale wetten over mensenrechten, is het gebruik van sommige tools die je helpen met het beschermen van je privacy in sommige gevallen (landen) illegaal. Verschillende van de privacy-tools die we in dit handboek bespreken zijn versleutelingstools. Die encryptie kan in sommige landen illegaal zijn of het kan zijn dat je er een licentie voor nodig hebt. Het gaat bijvoorbeeld om de landen China, Cuba, Iran, Libië, Maleisië, Noord-Korea, Singapore, Sudan, en Syrië. Als je in een aantal van deze landen binnenkomt, kan het zijn dat je moet melden dat je encryptietechnologie op je laptop hebt staan. Je moet overwegen welke juridische implicaties het gebruik van versleuteling dan heeft en weloverwogen besluiten nemen over waar en wanneer het veilig is om de software te gebruiken. Hier vind je meer over de wetten over encryptie in verschillende landen: www.cryptolaw.org.

In kaart brengen van gevaren
Er is veel informatie in dit handboek te vinden over verschillende gevaren en maatregelen die je kunt nemen om je tegen gevaren te verdedigen. Maar omdat de aanvalstechnologieën steeds veranderen en veel van de methodes volledig geheim zijn, kunnen we nauwelijks met enige betrouwbaarheid zeggen wat de exacte gevaren zijn, wanneer, waar en op wie ze van toepassing zijn, noch over de

effectiviteit van de verdediging. Daarom is het van belang dat je zelf een persoonlijke risicoanalyse uitvoert en op basis daarvan passende verdedigingsmaatregelen ontwerpt, terwijl je dit boek doorleest en de instructies toepast.

Het is ook verstandig een aantal praktische zaken daarin mee te nemen – sommige gebruikers compromitteren hun infosec om tegemoet te komen aan praktische wensen en eisen in hun dagelijkse werk, terwijl ze zich bewust zijn van de risico's. Dit terwijl andere gebruikers uitgekiende infosec toepassen die meer is dan ze eigenlijk nodig hebben, simpelweg omdat ze het voldoende eenvoudig in het gebruik vinden.

Een paar basisvragen die je jezelf moet stellen als je het gevaar rondom infosec in kaart wilt brengen, zijn:

1. Wie kunnen je tegenstanders of mogelijke aanvallers zijn?
2. Over welke hulpmiddelen zouden mogelijke aanvallers kunnen beschikken?
3. Hoe aannemelijk is het dat je potentiële aanvallers hun eigen tools tegen jou inzetten?
4. Welke risico's kunnen vanuit een gerichte aanval ontstaan voor jou en degenen met wie je communiceert en werkt?
5. Welke risico's kunnen ontstaan door passieve surveillance en hoe uitgebreid zijn de tools die worden gebruikt in een passieve surveillance?
6. Welke strategieën voor bescherming zijn praktisch, veilig en effectief in relatie tot het geschatte risico?
7. Welke strategieën zijn praktisch, veilig, effectief en te instrueren aan bronnen en collega's in relatie tot het ingeschatte risico en/of de risico's die ontstaan door de onderlinge communicatie?

Blijf op de hoogte

De gevaren veranderen door de tijd, maar dat geldt ook voor de technologieën die journalisten en burgers ter bescherming staan. Het is dus belangrijk infosec in theorie te begrijpen en steeds op de hoogte te blijven van actualiteiten rondom het toepassen van infosec in de praktijk. Raadpleeg bijvoorbeeld regelmatig de informatie en van Bits of Freedom (Nederlands) en van https://ssd.eff.org/en (Engels)

Hoofdstuk 1: systeembescherming

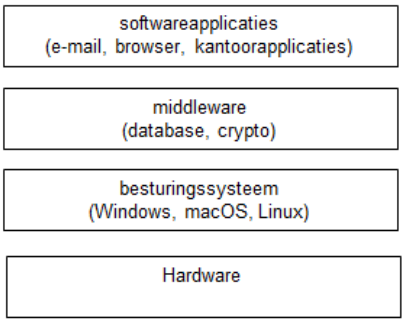
Afhankelijk van de specifieke risico's en de expertise van je belager, variëren de strategieën voor bescherming van eenvoudigweg je laptop of telefoon steeds bij je te houden tot het gebruiken van een tweedehands, contant betaalde laptop waarop je consistent robuuste informatiebeveiliging toepast gedurende een specifiek project. Maar de methodes die je gebruikt voor zijn alleen effectief als ieder onderdeel van je apparaat veilig is. Je kunt e-mails versturen met niet te kraken encryptie of de sterkst mogelijke wachtwoorden gebruiken, maar als je computer of apparaat is gecompromitteerd, gehackt of als deze kwetsbaar is, zijn al je inspanningen voor niets. Je encryptie kan dan eenvoudig kan worden omzeild zonder dat de code hoeft te worden gebroken. Je moet het beschermen van je systeem zien als een kaartenhuis: als het wil werken moet je de beveiliging vanaf een goed fundament opbouwen. In dit hoofdstuk leer je hoe je het fundament van een veilig systeem kunt bouwen door te leren omgaan met de beveiliging van je hardware en firmware (firmware is software die in de hardware is geprogrammeerd, vaak de besturingssoftware).

Dit hoofdstuk is ook meteen het belangrijkste hoofdstuk van het boek. Het is vrij technisch en bevat de meest uitdagende informatie van het boek. Er zijn veel oplossingen te geven, maar ultieme beveiliging is het resultaat van maar één daarvan. We laten je de realiteit zien van de kwetsbaarheden die je in hardware aantreft en laten het aan jezelf over om te beslissen wat de juiste beveiligingsmaatregel in jouw geval is. Voor sommige oplossingen die worden beschreven (zoals gespecialiseerde wijzigingen aan hardware en de vervanging van firmware), heb je hulp nodig van een professional. Maar ook al is het hoofdstuk wat lang en technisch, lees vooral door! Het is van belang dat je je bewust bent van de kwetsbaarheden in je eigen systeem, ook als je ze zelf niet kunt oplossen of niet de behoefte hebt om ze direct op te lossen. We geven je belangrijke informatie die je vertrouwen in het gebruik van je systeem richting zal geven en je voorbereidt op de toekomst waarin, naar wij hopen, op korte termijn eenvoudiger oplossingen worden ontwikkeld.

Generiek computermodel

Definities

- Interface - beeldscherm
- Applicaties – je software/programma's
- Middleware – kleefprogramma's die vaak twee verschillende, al bestaande programma's aan elkaar lijmen, oftewel die programma's toegang tot databases toestaan
- Operating System – Windows XP/7/8/10, macOS, Linux, etc.
- Firmware – op hardware geprogrammeerde basissoftware die instructies geeft over hoe het apparaat moet communiceren met de andere hardware van het apparaat
- Hardware – de fysieke onderdelen die samen een computer vormen



In dit hoofdstuk focussen we ons in eerste instantie op veiligheid op het meest fundamentele niveau: hardware en firmware.

Hardware en firmware

In dit hoofdstuk wordt uitgelegd hoe je aan veilige hardware komt en hoe je die veilig houdt. Je hoeft alleen te kiezen welk risiconiveau bij je past/wilt gebruiken voor jezelf en vervolgens de bijbehorende stappen te zetten.

De term 'Hardware' die we hier gebruiken, verwijst naar je fysieke apparaat. Voor belangrijke journalistiek raden we desktops af: ze zijn niet mobiel en niet alleen onpraktisch, maar ook kwetsbaar voor fysieke interventie als je niet in de buurt bent. We bespreken daarom alleen het gebruik van laptops in dit handboek. Als we het over de laptop hebben, bedoelen we alle fysieke onderdelen inclusief de accu, de harddisk-drive, cd-drive, wifikaart, microfoon en webcam. Ook kijken we naar hardware die je met je laptop kunt verbinden, zoals een willekeurig toetsenbord, muis, scanner/printer, webcam, etc.

Gevaren voor je hardware kunnen zijn:

- diefstal of beschadiging;
- fysieke aanvallen;
- virtuele aanvallen/aanvallen op afstand.

Het grootste risico voor je hardware is de kans op diefstal of beschadiging, de kans dat er fysiek mee wordt gerommeld of de kans dat de laptop virtueel, op afstand wordt benaderd om gegevens te verzenden (om gegevens te verzamelen en op te slaan).

We bespreken in dit hoofdstuk vijf belangrijke maatregelen voor het beschermen van je hardware:

Het voorkomen van virtuele en fysieke aanvallen op je hardware

1. koop de juiste laptop
2. pas de hardware aan

Het voorkomen van fysieke aanvallen op je hardware

3. koop je laptop anoniem
4. bewaak je laptop
5. neem detectiemaatregelen (voor het geval je van je laptop wordt gescheiden)

Misschien lijken deze vijf stappen op het eerste gezicht moeilijk, laat je niet uit het veld slaan. Ze zijn volledig uitvoerbaar door journalisten die niet bekend zijn met IT en informatiebeveiliging.

Het voorkomen van aanvallen op je hardware

1. Het kopen van de juiste laptop en risiconiveaus

De laptop die je aanschaft, bepaalt het maximaal bereikbare veiligheidsniveau. Nu we, door de documenten van Snowden, meer weten over de uitgebreide surveillancecapaciteiten, weten we ook welke apparaten wel en niet te beveiligen zijn. Hopelijk kunnen er in de toekomst meer veilige oplossingen worden ontwikkeld, maar helaas zijn er op dit moment slechts een aantal laptops volledig te beveiligen tegen de grootste bedreigingen.

Dit hoeft geen probleem voor jou of je bron te zijn, afhankelijk van met welk gevaar, met welke kwaadwillende je te maken hebt. Als je je communicatie en data moet beschermen tegen een

machtige overheid of bondgenoot (in de praktijk kunnen dat bijvoorbeeld belangrijke banken of invloedrijke bedrijven zijn), dan heb je een uitstekende beveiliging van je laptop(s) nodig. In andere gevallen moet je inschatten hoe geraffineerd de middelen van de kwaadwillende zijn, of het nu gaat om grote bedrijven, politieke, militaire of terroristische groepen, private beveiligingsbedrijven of specifieke individuen. Ook moet je inschatten hoe gemakkelijk die middelen tegen je zijn in te zetten, hoe belangrijk je als doel bent en welke maatregelen je in relatie daarmee wilt nemen.

Je moet met vier punten rekening houden als je een laptop koopt, omdat deze bepalend zijn voor de maximaal te bereiken mate van beveiliging van de laptop. Het gaat om: de onderhoudsmogelijkheid van de hardware, firmware, chipsets en het besturingssysteem

Onderhoudsmogelijkheid hardware
Kies bij voorkeur een laptop waarvan je de behuizing kunt openschroeven. Je kunt dan wat basisonderhoud aan de hardware doen en kiezen welke onderdelen je wilt houden of uitschakelen. Laptops van de merken IBM/Lenovo, HP, en Dell zijn vaak geschikt en verstrekken uitgebreide documentatie over de hardware op hun websites die behulpzaam kan zijn bij zelf uitgevoerde hardware-aanpassingen[1].

De behuizing van een MacBook is niet gemakkelijk te openen. Hiervoor heb je een behoorlijke vaardigheid nodig. Kun je dit, houd er dan rekening mee dat hardware-onderhoud ertoe kan leiden dat de garantie vervalt.

Firmware
Firmware is de software die op je laptop is geprogrammeerd in het diepe basisniveau. Kort gezegd geeft firmware de instructies over hoe de verschillende computeronderdelen met elkaar moeten communiceren. Firmware is te gebruiken als aanvalspunt, omdat hackers met voldoende vaardigheden (hoogstwaarschijnlijk overheidsniveau, zie hierna voor de risiconiveaus) in staat zijn om op afstand toegang te krijgen en op deze manier met prioriteit controle over je laptop kunnen krijgen. Dit ondermijnt uiteraard alle stappen die je zet om de laptop te beveiligen.

De firmware van je MacBook kun je op slot zetten, “locken”, zodat de firmware alleen nog toegankelijk is via een wachtwoord dat je zelf instelt. De mogelijkheid om die firmware op een Mac te locken, betekent een bijzonder beveiligingsvoordeel ten opzichte van andere laptops. Daarvan is namelijk slechts een beperkt deel van de beschikbare modellen te beveiligen door de originele, onwijzigbare firmware (eigendom van de leverancier; de code is niet openbaar of te wijzigen) te vervangen door opensourcefirmware. Die opensourcefirmware, Coreboot genaamd, is gratis voor iedereen en gebruikt openbare, wijzigbare code. Natuurlijk moet je bedenken dat vertrouwen in de veiligheid die het MacBook biedt via de lock ook afhangt van je vertrouwen in Apple. Aan de andere kant hangt het vertrouwen in Coreboot af van het vertrouwen in degene die de code wijzigt. In ieder geval zijn er geen kwetsbaarheden bekend in de firmwarelock en het gebruik ervan kan ervoor zorgen dat het hacken meer moeite kost.

De optie om Mac-firmware te locken is eenvoudig in gebruik en hij zorgt voor een behoorlijke muur van beveiliging zorgt tegen firmwarehacks. In verband daarmee zullen Mac-gebruikers van

[1] De genoemde flexibiliteit en documentatie is ook beschikbaar van andere merken – de suggesties die hierboven zijn gedaan, zijn geen aanbevelingen voor de genoemde merken of hun producten.

verschillende risiconiveaus de lock willen gebruiken. Om de firmwarelock in te stellen op je Mac (macOS): start de laptop op en houd de toets 'cmd' en de 'R' ingedrukt, zodat de laptop opstart in herstelmodus. Ga in bovenste menubalk naar 'Utilities' → 'Firmware Password Utility' → 'Turn On Firmware Password'. Kies een sterk wachtwoord (zie hoofdstuk 8) en klik op 'Set Password'. Het is erg belangrijk dat je dit wachtwoord onthoudt, omdat je anders de toegang tot je Mac kunt kwijtraken.

Chipsets
Sinds rond 2006 plaatst Intel speciale onderdelen in hun chipsets (chipsets zijn combinaties van chips die samenwerken op het moederbord van de laptop). Hiermee wordt een geautomatiseerd management van systemen over een netwerk mogelijk. Deze technologie is de zogenaamde 'Intel Active Management Technology' (AMT), en het stelt bijvoorbeeld een IT-technicus in staat om binnen het netwerk van een groot kantoor of universiteit, software te updaten of andere dingen uit te voeren op apparaten zonder dat die fysiek in de buurt hoeven te zijn. De functionaliteit is niet alleen handig; het probleem met deze technologie is dat deze kan worden misbruikt om spyware te installeren of het systeem op andere wijze te manipuleren. Alle laptops die na 2008 zijn gemaakt, hebben de speciale AMT-chipsets en zijn daarom kwetsbaar voor deze aanvalsmogelijkheden als ze in een netwerk zijn aangemeld.

De chipset versie 'Intel 945' is de laatste chipset zonder deze functie (een "pre-AMT-chipset") en die leent zich dus goed voor een te beveiligen moederbord/computer. Als je een laptop uitkiest, kun je op de specificatie van het apparaat zien welke chipset wordt gebruikt.

Besturingssysteem
We weten dat inlichtingendiensten vaak toegang hebben tot besturingssystemen via zogenaamde 'backdoors', achterdeurtjes, waardoor ze toegang tot je gebruikersdata kunnen krijgen. Om erop te kunnen vertrouwen dat je besturingssysteem geen potentiële achterdeurtjes heeft (en dus niet voor surveillancedoeleinden kan worden gebruikt), moet het systeem open source zijn. Het is daarom verstandig om een laptop te kopen waarop je zelf een besturingssysteem kunt installeren. Dat besturingssysteem is dus bij voorkeur open source, waarbij de broncode publiek en gratis is. Op de meeste laptops is het vrij eenvoudig om een ander besturingssysteem te installeren en te gebruiken dan die is voorgeïnstalleerd. Dat is niet het geval bij een MacBook, zie hierna.

Je hebt verschillende mogelijkheden om een ander besturingssysteem te gebruiken. Zo kun je een voorgeïnstalleerd besturingssysteem volledig verwijderen en een nieuwe installeren, of je gebruikt een virtuele machine of 'sandbox' op het voorgeïnstalleerde systeem. Hierdoor gebruik je in feite meerdere besturingssystemen tegelijkertijd. De broncode van besturingssystemen waarop een eigendomsrecht van de leverancier zit (Windows, Mac), zijn niet openbaar en hebben wellicht verschillende ingebouwde achterdeuren, al dan niet bewust aangebracht. Het is daarom niet bekend hoeveel veiligheid tegelijkertijd gebruikte besturingssystemen echt bieden.

Het voorgeïnstalleerde besturingssysteem kan van de meeste laptops gemakkelijk worden verwijderd. Het is niet aan te raden een besturingssysteem van een Mac te verwijderen, omdat dit negatieve invloed kan hebben op de werking van het complete systeem. Het is weliswaar mogelijk om verschillende besturingssystemen op een Mac te gebruiken, maar daarvoor heb je kennis nodig over hoe je een 'virtual machine' moet draaien. Daar gaan we om eerdergenoemde reden veiligheidsredenen verder niet op in. Als alternatief kun je het besturingssysteem 'Tails' gebruiken op een Mac. Deze werkt buiten de harddrive om en draait vanaf een USB-drive (zie hoofdstuk 2). Het besturingssysteem wordt uitgebreid besproken in hoofdstuk 2.

Risiconiveaus en laptop

Hoe moet je nu deze vier fundamentele veiligheidspunten interpreteren naar je eigen risiconiveau? Het op afstand verkrijgen van toegang tot hardware, firmware en chipsets is waarschijnlijk alleen mogelijk door inlichtingendiensten of technologisch geavanceerde landen. Maar alle technologie wordt door de tijd heen gemakkelijker toegankelijk voor minder machtige groepen. Als je een inlichtingendienst als kwaadwillende kunt aanmerken, is het verstandig de genoemde kwetsbaarheden mee te nemen bij de keuze van je laptop. Zelfs als je niet te maken hebt met een dergelijk hoog risicofactor, is het verstandig om voorzorgsmaatregelen te nemen voor je veiligheid (vooral de maatregelen die weinig moeite kosten, zoals het locken van de firmware op een Mac).

Het is aannemelijk dat technologisch geavanceerde inlichtingendiensten toegang hebben tot besturingssystemen via achterdeurtjes. Daarnaast is het aannemelijk dat grote of machtige bedrijven de benodigde informatie in bezit kunnen krijgen om die toegang te bewerkstelligen. Dus, als in jouw geval een groot bedrijf de kwaadwillende is, moet je de afwegen wat dit voor de keuze van besturingssysteem kan betekenen. De laptopkeuze is dus niet gemakkelijk. Je moet de tijd nemen om de informatie door te nemen, om zo weloverwogen te kunnen bepalen met welk risiconiveau je te maken hebt en te beslissen hoeveel moeite en discipline je wilt steken in je informatiebeveiliging.

Hieronder vind je een aantal suggesties voor te kopen laptops in de vier algemene risiconiveaus (laag, middelmatig, hoog, top):

- **laag risico**: *sleepnet, ook wel dragnet, (algemene) surveillance, laag niveau individueel hacken, diefstal* | Je kunt beginnen met een willekeurige laptop. De meeste systemen zijn redelijk goed te beveiligen tegen de gewone bedreigingen op softwareniveau. Verder kun je jezelf beschermen door je laptop steeds bij je te houden, zodat er geen fysieke interventie of diefstal kan plaatsvinden. Je kunt zo ook de digitale dragnet via software en applicatiekeuze vermijden. Een goede onderzoeksjournalist is dit niveau snel ontgroeid.

- **middelmatig risico**: *gerichte surveillance, door een kwaadwillende die voorbereid is of de mogelijkheid heeft om vrij onbeperkt middelen in te zetten* | Gebruik een laptop waarvan je het voorgeïnstalleerde besturingssysteem kunt verwijderen om je eigen te installeren (bij voorkeur een opensource Linux-systeem), of gebruik het Tails-besturingssysteem vanaf USB op een willekeurige computer. Zie hoofdstuk twee voor uitgebreide informatie over besturingssystemen.

- **Hoog risico**: *gerichte surveillance door een inlichtingendienst* | Er is maar een handvol apparaten die op een betrouwbare manier te beveiligen zijn tegen het op afstand benaderen van hardware, firmware en chipset. Sinds 2014 worden de modellen IBM ThinkPad X60 en X60s het meest op deze manier beveiligd. Die laptops hebben een Intel 945-chipset (een pre-AMT-chipset) en er kan specialistisch werk worden gedaan om de hardware en firmware te beveiligen. De oorspronkelijke firmware kan door opensourcefirmware (Coreboot) worden vervangen. Vervolgens maak je gebruik van het Tails-besturingssysteem (zie hoofdstuk 2) op de beveiligde laptop, om zo de veiligheid van het systeem in stand te houden.
  Als je zo'n laptop nodig hebt, neem dan op veilige manier contact op met het Centre for Investigative Journalism. Je kunt een versleutelde e-mail sturen naar infosec@tcij.org of contact opnemen met het kantoor (http://www.tcij.org/about-cij/contact-cij). Wil je het zelf doen, dan kun je het beste een laptop kopen met een pre-AMT chipset, waarvan je de behuizing kunt openmaken. Gebruik onlinedocumentatie om te bekijken hoe je het basisonderhoud aan de

hardware moet uitvoeren. Je kunt bijvoorbeeld de harddrive, de microfoon, webcam, wifikaart, bluetoothkaart, 3/4G-modem en ethernetpoort verwijderen (zie punt 2 in dit hoofdstuk). Houd wel in gedachten dat je hierin getraind moet zijn, anders lukt het niet om de firmware te vervangen of de ingewikkelde hardware-aanpassingen uit te voeren voor topveiligheid.

- **toprisico**: *gerichte, gestuurde surveillance door een inlichtingendienst* | In situaties met een zeer hoog risico moet je ervoor zorgen dat je ten minste twee laptops hebt waarop alle genoemde beveiligingsmaatregelen zijn uitgevoerd. Eén van beide moet nooit, onder geen enkel beding met het internet worden verbonden. Dat is je "airgap-laptop": een laptop die nooit ofte nimmer online gaat. Dit apparaat is bruikbaar voor het opslaan en benaderen van bestanden (bijvoorbeeld die je op een USB-stick hebt staan), voor het schrijven van artikelen en het maken van verslagen. Jij of de specialist die je helpt, verwijdert alle onderdelen die met connectie met internet te maken hebben of maakt deze onbruikbaar om je ervan te verzekeren dat de laptop daadwerkelijk offline is en blijft (zie punt 2 hierna). Je laptops zijn bij voorkeur allebei speciaal beveiligde IBM ThinkPad X60s. Feit: Glenn Greenwald gebruikte een airgap-laptop om met de Snowden-documenten te werken.

  De airgap voegt een extra niveau van veiligheid toe aan de data van jou of jouw bron, omdat je belangrijke documenten niet alleen op een beveiligd apparaat opslaat, maar omdat het apparaat ook volledig offline blijft. Zelfs de best beveiligde laptop staat bloot aan een bepaalde mate van risico als het online gaat, in het bijzonder als de gebruiker ervan het onderwerp van een gestuurde aanval is.

2. Aanpassen van je hardware

We kijken naar de te wijzigen onderdelen in de laptop die gebruikt kunnen worden om jou, je bron en je werk in de gaten te houden:

- webcam
- microfoon
- harddiskdrive
- wifikaart
- bluetoothkaart
- 3/4G-modem
- ethernetpoort

Webcam
Webcams kunnen niet alleen in het geheim op afstand worden bediend voor specifieke doelen, ook de beelden die met de webcam worden genomen, kunnen worden opgevangen als onderdeel van algemene surveillanceprogramma's (dragnet), bekijk Snowden revelation of GCHQ's OPTIC NERVE program). Een eenvoudige oplossing: plak een sticker of webcamcover over je webcam.

Microfoon
Ook de microfoon van je laptop kan in het geheim op afstand worden geactiveerd om audio op te vangen. Je kunt hete lijm over het microfoon-inputkanaal van de laptop doen om het geluid te dempen. Beter is de behuizing te openen en de draad van de microfoon door te snijden.

Harddiskdrive
Het is gebleken dat sommige harddiskdrives gebruikmaken van slechte firmware. Deze kan worden geactiveerd om jouw computerbeveiliging te compromitteren in het geval je een doelwit wordt van een dienst met een slimme toolkit.

Als je te maken hebt met een hoog risiconiveau, is het aan te raden om de harddiskdrive te verwijderen en te werken met USB-drives. Die zijn bovendien ideaal voor opslag van het zeer veilige besturingssysteem Tails (zie hoofdstuk 2): op zo'n drive kun je een klein, geanonimiseerd besturingssysteem gebruiken waarmee je kunt werken. USB-sticks zijn gemakkelijk mee te nemen, te kopiëren (om met collega's of bronnen te delen) en ze zijn gemakkelijk te beschermen met sterke encryptie (zie hoofdstuk 4). Dat betekent bovendien dat je data veilig op je USB-stick beschikbaar blijft, zelfs als je laptop wordt gestolen. Het kan natuurlijk ook zijn dat je de harddiskdrive wilt houden voor je gewone werk en dat je met USB-drives (al dan niet met Tails) werkt voor specifieke projecten.

Wifi en bluetoothkaart, 3G modem

Ieder onderdeel van je laptop dat connectie kan maken met een ander apparaat, kan in het geheim op afstand worden benaderd om bijvoorbeeld surveillancetools te installeren of om jouw data naar een tegenstander te sturen. Heb je te maken met een hoog risiconiveau, zorg er dan voor dat je zoveel mogelijk controle over de connectiviteit van je laptop hebt.

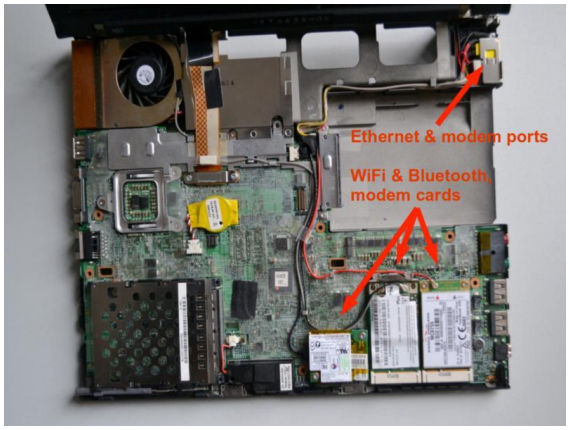
De beste manier om dat te bewerkstelligen is het fysiek verwijderen van de componenten die connectie kunnen maken. Dat betekent dat je de behuizing moet openmaken en de wifikaart, de bluetoothkaart en het 3/4G-modem moet losschroeven als je laptop die heeft. Als je niet precies weet hoe dat moet, kijk dan in het handboek van je laptop: vaak kun je die online gemakkelijk vinden. Het voelt in eerste instantie misschien als een uitdagende taak, maar iedereen met een vaste hand en goede instructie kan dit gemakkelijk doen, ook als het voor het eerst is.

Nu heb je er controle over wanneer je online en offline bent. Je kunt bijvoorbeeld een USB-adapter met wifimogelijkheid kopen die op dezelfde manier werkt als de ingebouwde wifikaart. Zo kun je toch online gaan. Het verschil is dat je de adapter gemakkelijk kunt aansluiten en verwijderen van de USB-poort. Zo beslis je zelf wanneer je online en offline bent. Als alternatief kun je online gaan met behulp van een ethernetkabel.

Ethernetpoort

Met de ethernetpoort kun je de laptop fysiek (met een kabel) verbinden met een Local Area Network (LAN). Dat kan een netwerk in een groot kantoor zijn of een router thuis van je internetprovider. Tegenwoordig is wifi overigens meer algemeen geworden dan bekabelde internetconnecties.

Ethernetpoorten hebben specifieke kwetsbaarheden die gebruikt kunnen worden tegen vooral doelwitten van hoog risiconiveau. Om je apparaat te beschermen tegen misbruik van je apparaat via de ethernetpoort, bijvoorbeeld van je airgap-laptop, kun je de poort met hete lijm vullen. Als alternatief kun je de poortbedrading binnen de behuizing van de laptop doorknippen.



3. Je laptop anoniem kopen

Nu je meer weet over informatiebeveiliging, wil je wellicht een of twee nieuwe laptops aanschaffen. Dat is niet alleen een verstandige beslissing als je werkt met een bron van hoog risico of als je aan een gevoelig project werkt. Het is ook verstandig om jezelf voor te bereiden op de mogelijkheid van situaties die zich kunnen voordoen, zodat je het geleerde kunt toepassen als dat nodig is. Nadat je dit hoofdstuk hebt gelezen, bepaal je wat voor model laptop je wilt kopen. Onderzoek ook hoe je de anonieme Tor-browser (zie hoofdstuk 3) moet gebruiken, voordat je de laptop via Tor koopt.

Het risiconiveau van je bron = jouw risiconiveau
Als je als journalist werkt met iemand van een hoog risiconiveau, bijvoorbeeld een klokkenluider van een inlichtingendienst, dan is de kans aanwezig dat deze persoon al wordt gesurveilleerd. Je moet aannemen dat het surveillancerisico van je bron daarmee ook op jou van toepassing is.

Anonimiteit bij aankoop
Het is belangrijk om het aankoopproces van de laptop zo anoniem mogelijk te laten verlopen als je te maken hebt met een hoog risiconiveau. Daarmee voorkom je dat een kwaadwillende de kans krijgt van tevoren surveillancetools in de hardware te installeren. Als een tegenstander in de gaten heeft dat je nieuwe hardware aanschaft, is de kans aanwezig dat deze probeert om na de aankoop fysiek of virtueel op het apparaat in te breken of de laptop te volgen zodat deze naar jou of je bron leidt. De Snowden-documenten onthulden namelijk dat inlichtingendiensten apparaten zoals laptops, telefoons en andere elektronica onderscheppen tijdens het verkoopproces, zodat er surveillancemiddelen in kunnen worden aangebracht voordat (of nadat) de leverancier de verzenddoos sluit en op transport doet. Je moet daarom geen hardware online kopen (ook geen opladers). De meeste hardware-elementen kunnen worden aangepast om ze als surveillancetool in te zetten.

Wil je echt zeker zijn van anonimiteit, overweeg dan om de laptop in persoon te kopen en betaal contant. Mocht je een ouder model kopen, zoek dan ergens een elektronicawinkel met tweedehands spullen (bij voorkeur niet in de buurt van waar je normaal gesproken winkelt). Als je te maken hebt met een hoog risiconiveau is het verstandig om elke laptop en de accessoires (zoals USB-sticks) in verschillende winkels te kopen. Terwijl je winkelt, laat je je apparaten die getrackt kunnen worden (zoals je telefoon) op een veilige plek thuis, of je doet ze in een Faraday-bag (een metalen omhulsel dat signaaltransmissie voorkomt).

Voor media- en campagneorganisaties is het aan te raden om het materiaal als voorzorgsmaatregel van tevoren te beveiligen (en het in een kluis te bewaren tot het moment van gebruik). Vervolgens leer je je personeel ermee werken. Voor advies over kant-en-klare toolkits, neem contact op met infosec@tcij.org.

4. Je laptop bewaken

Als je het risico loopt dat je in de gaten wordt gehouden, moet je belangrijk nieuw gedrag aanleren: om diefstal (bewuste of toevallige) of fysieke aanvallen op je hardware te voorkomen houd je je laptop altijd bij je of je houdt deze binnen je blikveld. Het aanleren van dergelijk gedrag wordt wel ‘OpSec’ genoemd, Operational Security.

Als je laptop op enig moment onbeheerd achterblijft (bijvoorbeeld thuis, in een café of op kantoor) of kort in het bezit van iemand anders is (bijvoorbeeld bij het inchecken van bagage voor een vlucht, of

als het wordt ingenomen door politie/autoriteiten), dan moet je je afvragen of de mogelijkheid bestaat dat je systeem in de tussentijd is gecompromitteerd. Die kans hangt natuurlijk samen met het risiconiveau. Snowden ontwikkelde overigens in 2017 de app 'Haven' die voor OpSec kan worden ingezet.

Zorg ervoor dat jouw veilige laptop simpel, klein en zo licht mogelijk is. Voorkom dat de laptop wordt verbonden met een muis, toetsenbord, docking station of andere apparaten (het is aannemelijk dat ermee is gerommeld in het geval van een hoog risiconiveau). Zo beperk je de hardware die je met je meeneemt en/of waar je verantwoordelijk voor bent.

Je moet niet alleen kijken naar de fysieke veiligheid van je hardware op dit moment of op enig moment in de toekomst. Het is ook belangrijk terug te kijken. Vraag je af of de hardware eerder fysiek aangevallen kan zijn. Hoe is het gemaakt, kan de hardware al gecompromitteerd zijn?

We hebben al besproken dat het verstandig is nieuwe hardware in persoon te kopen, met contant geld, omdat we weten dat de hardware tijdens verzending risico loopt. Dit maakt het niet alleen mogelijk een laptop anoniem aan te schaffen, je kunt ook meteen de fysieke verantwoordelijkheid voor je rekening nemen.

5. Detectiemaatregelen

Het is erg moeilijk om te achterhalen of er een fysieke ingreep aan je laptop is uitgevoerd. Als je je laptop veilig moet opbergen om wat voor reden dan ook (bijvoorbeeld als je de grens van een bepaald land wilt passeren zonder je laptop), dan moet je dat op zo'n manier proberen te doen, dat je het later kunt zien als er iemand in de tussentijd aan heeft gezeten. Snowden ontwikkelde in 2017 de app 'Haven' die voor OpSec kan worden ingezet. Wees creatief, maar het zal een uitdaging zijn om slimmer te zijn dan een vaardige tegenstander. Bij voorkeur laat je de laptop in bescherming achter bij iemand die je vertrouwt, als je het apparaat zelf niet kunt bewaken.

Als technologische verdediging bij lage risiconiveaus en als algemeen veiligheidsmaatregel kun je de opensource-applicatie Prey downloaden. Dit is trackingsoftware die je helpt je apparaat te vinden, te locken en terug te krijgen. Je kunt ook screenshots maken met het gestolen apparaat en de webcam activeren om een foto te maken van degene die het in zijn bezit heeft. Het downloaden van trackingsoftware voelt misschien wat tegengesteld voor een journalist die juist zijn privacy wil beschermen, maar omdat de applicatie open source is, wordt het beschouwd als redelijk veilig. Maar een slimme tegenstander trapt niet in deze valkuil. Het is aan te raden dat je deze software alleen gebruikt als verdediging tegen minder vaardige tegenstanders.

Als je hardware wilt blijven gebruiken die niet te beveiligen is, kun je nog steeds maatregelen nemen om je data en communicatie te beveiligen tegen minder sterke surveillanceactiviteiten. Lees dus zeker door, maar wees je ervan bewust dat het een fait accompli is als iemand met voldoende mogelijkheden, capaciteiten en motivatie je data wil verkrijgen als je een surveillancedoel wordt.

Hoofdstuk 2: besturingssysteem

Naast de firmware (zie hoofdstuk 1) is het besturingssysteem de belangrijkste software op een computer. Deze software bestuurt de computer als deze opstart en is de interface waarmee je je computer gebruikt. Kortom, het besturingssysteem vertelt de computer wat deze moet doen en hoe dat moet worden gedaan. Populaire besturingssystemen zijn versies van Windows (zoals XP, Vista, 8, 10), Mac (macOS) en Linux-versies (Ubuntu, Mint).

Gevaren in relatie tot besturingssystemen

- malware, virussen;
- surveillanceachterdeurtjes in een besturingssysteem, toegankelijk voor de inlichtingendiensten.

Twee hoofdmaatregelen ter bescherming van je besturingssysteem

- gebruik een opensourcebesturingssysteem (voor een middelmatig risiconiveau), bijvoorbeeld Ubuntu of Mint (Linux);
- gebruik Tails, een opensourcebesturingssysteem dat incognito en onvindbaar blijft (hoog tot top risiconiveau).

Opensourcebesturingssystemen

Computers die draaien op besturingssystemen van Microsoft en Apple (dus Windows, macOS) maken gebruik van software met beschermde broncode. Van deze besturingssystemen is het aannemelijk dat ze surveillanceachterdeurtjes hebben en houden die toegankelijk zijn voor GCHQ, de NSA en aanverwante partijen die er belang bij hebben. Het besturingssysteem van Microsoft is in het bijzonder ongeschikt, omdat er meer van de broncode beschermd is dan die van Apple. Bovendien zijn besturingssystemen van Microsoft gevoeliger voor malware en virussen. Kortom, systemen met gesloten sourcesoftware zijn ongeschikt voor systemen met belangrijke data en communicatie en/of als je denkt dat jij of iemand met wie je communiceert een surveillancedoelwit is of verwacht te worden. Gebruik dus een opensourcebesturingssysteem als je met dit risiconiveau te maken hebt.

Opensourcesoftware

Opensourcesoftware is gratis gedistribueerde software waarvan de broncode – de code waarmee het systeem is gemaakt – publiek en open, inzichtelijk is. Hierdoor kan een onafhankelijke expert op ieder willekeurig moment de broncode bekijken en zich ervan vergewissen dat er geen beveiligingsfouten in de bouw van het besturingssysteem zitten. Een volledige definitie in tien punten van open source is beschikbaar op www.opensource.org/osd (Engels).

Verder zijn opensourcebesturingssystemen minder kwetsbaar voor malware (kwaadaardige software, vaak spyware) en virussen. Dat komt omdat ze veel minder worden gebruikt dan besturingssystemen van een fabrikant en daardoor in verhouding een laag marktaandeel hebben.

Opensourcesoftware is ook bekend als gratis software omdat de software gratis beschikbaar is/gedistribueerd wordt (op basis van vrijwillige donatie).

Als je hardware is beveiligd tegen geautomatiseerde en vooropgezette surveillance, is het van vitaal belang dat je geen software installeert die het systeem opnieuw kwetsbaar maakt. Zelfs als je met een laag risiconiveau te maken hebt, is het belangrijk om de juiste software te gebruiken ter beveiliging van je data en communicatie van geautomatiseerde surveillance op grote schaal (dragnet/sleepnet).

Je moet je er van bewust zijn dat opensourcesoftware net zo betrouwbaar is als het vertrouwen dat je stelt in de expertise en de frequentie waarmee de broncode is gebouwd en onderhouden/onderzocht. Echter, veelgebruikte opensourcesoftware wordt ook vaker onderzocht en heeft daarom de voorkeur boven software met niet openbare broncode (in ieder geval voor infosec). Kies daarom bijvoorbeeld voor LibreOffice in plaats van voor MS Office.

Noot: mobiele besturingssystemen met beschermde sourcesoftware zoals iOS en Android, zijn onontbeerlijk op smartphones en tablets. Die apparaten zijn daarom niet te beveiligen tegen gerichte aanvallen. Zie hoofdstuk 7 voor informatiebeveiliging van mobiele systemen.

Linux is het toonaangevende open source, community-ontwikkelde besturingssysteem. Je kunt uit veel verschillende versies van Linux-besturingssystemen kiezen. Wij behandelen de versie Ubuntu in het bijzonder omdat deze versie het meest gebruikte Linux-besturingssysteem is. Tegenwoordig wordt ook de versie Mint vaak gebruikt door Windows-gebruikers, omdat deze versie daar wat op lijkt.

1. Ubuntu (Linux-versie)

Ubuntu.com

Ubuntu is het meest gebruikte Linux-besturingssysteem. Het is gemakkelijk te installeren, zeer functioneel en redelijk gebruikersvriendelijk. Je kunt ervoor kiezen om je Windows-besturingssysteem te vervangen door Ubuntu, maar je kunt ook beide op dezelfde laptop draaien (dat kan fijn zijn als je eerst bekend wilt worden met het nieuwe systeem voordat je overstapt). Ubuntu is redelijk gebruikersvriendelijk en niet heel verschillend van andere besturingssystemen en daarom raden wij aan je Windows-systeem volledig te vervangen, omdat dit beter is voor je informatiebeveiliging. Immers, met het Windows-besturingssysteem blijven de mogelijke achterdeurtjes op je laptop staan. Let op dat je met het verwijderen van het oude besturingssysteem ook alle bestanden verwijdert die ermee zijn geassocieerd. Zorg er dus voor dat je een back-up maakt van alle bestanden die je wilt houden, voordat je het besturingssysteem verandert.

We raden onervaren gebruikers af om het besturingssysteem van MacBook te wissen om Ubuntu te installeren. Dit kan problemen veroorzaken met de functionaliteit van het apparaat. Voor een Mac kun je Ubuntu gebruiken via een zogenaamde virtuele machine. Hier gaan we verder niet op in omdat het niet duidelijk is welke veiligheidsvoordelen kunnen worden bereikt als er tegelijkertijd twee besturingssystemen draaien.

Let op; een paar onderdelen van Ubuntu gebruiken momenteel geslotensource-software. Er wordt aangenomen dat deze geen veiligheidsrisico vormen, alleen dat is niet met zekerheid te zeggen. Andere populaire versies van Linux, waaronder Debian en Trisquel, zijn volledig open source. Deze zijn alleen iets minder intuïtief in gebruik en onderhoud voor iemand die onbekend is met Linux.

2. Tails

tails.boum.org

Voor de grootste veiligheid gebruik je Tails: Tails is een niet te traceren, incognito besturingssysteem. De letters Tails betekenen 'The Amnesic Incognito Live System'. Het is een op Linux gebaseerd besturingssysteem (open source) en het beschermt de privacy en anonimiteit van de gebruikers.

Amnesic: omdat er geen enkel spoor van het systeem op je computer achterblijft nadat je het systeem hebt afgesloten/uitgezet.

Incognito: omdat het standaard is gericht op privacy en veiligheid als je het internet bezoekt en zo censuur kan omzeilen. Tails is speciaal ontworpen als anti-surveillancesysteem en het heeft verschillende ingebouwde op veiligheid gerichte applicaties (volledig open source).

Ingebouwde anonimiteit online
Op het moment dat je met het internet verbonden bent, zendt en ontvangt verschillende software op je computer met enige regelmaat datapakketjes via het internet, of je er nu actief gebruik van maakt of niet. We weten dat inlichtingendiensten deze netwerkactiviteit routinematig controleren en dit steeds verder intensiveren. Echter, alle software van Tails is ervoor geconfigureerd om anoniem verbinding met het internet te maken via Tor (zie hoofdstuk 3), en zo word je beschermd tegen netwerksurveillance.

De ingebouwde Tor-webbrowser heeft bovendien populaire extensies die de veiligheid vergroten, zoals HTTPS Encryption en HTTPS Everywhere. Dit zijn uitbreidingen (plug-ins) die je surfgegevens encrypten. Andere extensies in Tor: Adblock Plus om advertenties en tracking te voorkomen en NoScript om kwaadaardige JavaScript en Flash te blokkeren omdat deze je anonimiteit kunnen compromitteren. Als je Tails gebruikt met de hoogste veiligheidsinstellingen kan dat tot gevolg hebben dat sommige webfuncties niet werken, maar dat is een compromis die zeker de moeite waard is als je daarvoor een onnavolgbare goede privacy terugkrijgt wanneer je aan gevoelige projecten werkt. Als alternatief kun je de veiligheidsinstellingen lager zetten (in het Tor-veiligheidsscherm) of de "onveilige browser" van Tails gebruiken.

Noot: als je de onveilige browser gebruikt of als je via Tor inlogt in op een account die duidelijk aan jouw echte identiteit is gekoppeld, dan compromitteer je je anonimiteit gedurende de volledige Tails-sessie. Sluit Tails af en start deze opnieuw iedere keer als je een nieuwe identiteit gebruikt. Let op, ook bestanden en documenten kunnen metadata bevatten die jouw locatie via GPS onthullen. Bekijk hoofdstuk 4 voor tips over het verwijderen van dergelijke metadata.

Ingebouwde e-mail en chat met encryptie
Tails biedt een ingebouwde dienst voor chat en e-mail met encryptie. Tails bevat Icedove (Thunderbird) als e-mailprogramma met OpenPGP voor e-mailencryptie (zie hoofdstuk 5) en de instant-messenger Pidgin die privé en anoniem chatten ondersteunt.

Ingebouwde bestandsencryptie
Tails biedt bovendien LUKS waarmee je bestanden kunt versleutelen. Als je bestanden wilt opslaan op dezelfde USB-stick waarmee je Tails draait, kun je daarvoor een permanente bewaarplek op de stick aanmaken, een zogenaamd "persistent volume". Tails zal de bestanden op dit persistent volume standaard versleutelen, en steeds om je wachtwoord vragen voor toegang tot de opgeslagen bestanden.

Expert-info: het persistente volume is alleen bruikbaar voor de opslag van relatief onbelangrijke documenten en informatie, je moet het niet gebruiken om de meer gevoelige documenten mee te bewaren of mee te nemen. Het persistent volume is namelijk niet verborgen. Als iemand de USB-stick in handen krijgt, kan men zien dat er een volume met encryptie is aangemaakt op de stick. Dat kan erin resulteren dat ze je dwingen het wachtwoord te geven. Voor die gevoelige documenten moet je een verborgen volume ("hidden volume") aanmaken, eventueel op een andere USB-stick, die niet zichtbaar ruimte inneemt. Alleen jij weet dat het er is. Daarvoor kun je bijvoorbeeld heel goed VeraCrypt gebruiken (zie hoofdstuk 4).

Ingebouwde wachtwoordbeveiliging
Tails bevat de wachtwoordmanager KeePassX. Deze software slaat gebruikersnamen en wachtwoorden met encryptie op in een lokale database die weer wordt beschermd door een hoofdwachtwoord. Verder heeft Tails PWGen, een sterke wachtwoordgenerator. Zie hoofdstuk 8 voor het gebruik van wachtwoordmanagers.

Tails is ontworpen voor gebruik vanaf een USB-stick, onafhankelijk van het originele besturingssysteem van de computer. Dat betekent dat je de harddrivedisk van je laptop kunt verwijderen (aan te raden voor werk met een hoog risiconiveau) en deze vervolgens vanaf de USB-stick met Tails kunt opstarten. Daarnaast kun je de USB-stick met Tails in een computer doen waar de harddrivedisk nog in zit en dan opstarten met Tails. De computer zal het originele besturingssysteem en de harddrivedisk negeren en in plaats daarvan opstarten vanaf de USB-stick met Tails.

De beschikbaarheid van een systeem als Tails op een USB-stick is ideaal voor gevoelige journalistieke projecten. Je machine kan zo schoon blijven, zonder een spoor van je werk achter te laten en je documenten kunnen worden opgeslagen op een gemakkelijk mee te nemen, goedkope USB-stick. Tails heeft zelfs opensourcesoftware voorgeïnstalleerd waarmee je kunt bewerken, zoals:

- LibreOffice, waarmee je documenten kunt maken, lezen en wijzigen;
- PiTiVi om video's aan te passen;
- Audacity voor het bewerken van geluid.

De USB-stick is ideaal voor onderweg en je kunt het in iedere computer inpluggen als je de computer zo instelt dat deze vanaf de USB-stick met Tails opstart. Hoe dat moet wordt hieronder uitgelegd. Het is verstandig om voor verschillende projecten aparte USB-sticks met Tails te hebben, zodat je de sporen van je identiteit verspreidt en je een minimaal risico loopt als je een USB-stick verliest. In bepaalde gevallen kun je er ook voor kiezen om een kant-en-klare USB-stick met Tails aan je bron te geven met instructies. Op deze manier heeft de bron ook de mogelijkheid om veilig met je te communiceren. In situaties met een hoog risiconiveau kan het verstandig zijn om Tails te gebruiken op een ander apparaat dan je gebruikelijke laptop (airgap, zie hoofdstuk 1, toprisiconiveau).

Ubuntu is een prima optie voor dagelijks, niet-gevoelig werk. Toch is het verstandig een USB-stick met Tails te maken en deze te gebruiken als je aan de slag gaat met een gevoelig project, in het bijzonder als je met belangrijke documenten werkt, communiceert met personen op wie een hoog risiconiveau van toepassing is of als je gevoelige projecten online onderzoekt. Verder kunnen tijdige maatregelen op het gebied van informatiebeveiliging je helpen om je anonimiteit van tevoren te beschermen/bewaren, waarmee je tijd rekt voordat jij en je belangrijkste bron doelwit van surveillance worden.

Je weet nu hoe je je systeem op een robuuste manier kunt beschermen. In de volgende hoofdstukken leer je hoe je je communicatie kunt beschermen, hoe je je surfdata anonimiseert en hoe je gevoelige documenten moet versleutelen en meenemen.

Installatie Ubuntu

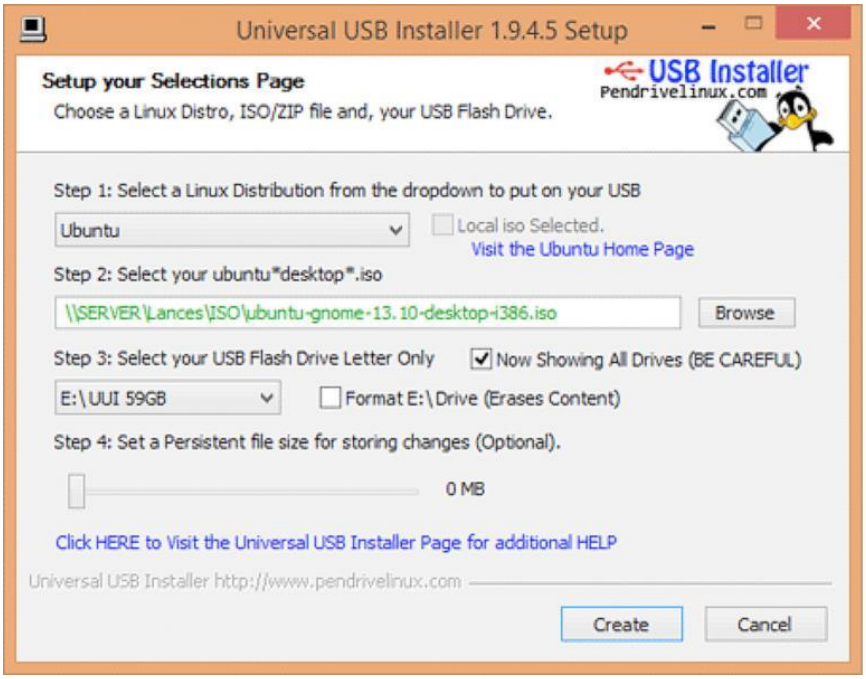
Noot: alle Windows-documenten, -programma's en –bestanden, etc. worden gedeletet als je Windows vervangt met Ubuntu (aanbevolen). Zorg dus voor een back-up van de bestanden die je wilt houden.

1. *Download Ubuntu*
   Download Ubuntu via www.ubuntu.com/download/desktop.
   Let op dat je de juiste versie downloadt. Hiervoor moet je weten hoeveel RAM je laptop heeft. Je downloadt of de 32-bit-versie (voor oudere apparaten, zoals de IBM ThinkPads met 2GB RAM of minder) of de 64-bit-versie (voor nieuwere apparaten met 4GB RAM of meer). De download kan wat tijd kosten (20 tot 60 minuten).

2. *Download de USB-installer voor Linux*
   Ga naar www.ubuntu.com/download/desktop/create-a-usb-stick-on-windows, click 'Download Pen Drive Linux's USB Installer ›', en scrol naar beneden. Klik op de grote knop met 'Download UUI'. Hiermee download je het USB-installatieprogramma, dat je op een USB-stick opslaat. Dat gebruik je vervolgens om Ubuntu mee te installeren. Je moet daarvoor Ubuntu eerst in het installatieprogramma laden (zie punt 3).

   Expert-info: tijdens de installatie kan de harddisk geen andere programma's draaien. Je hebt dus een andere bron nodig – in dit geval een USB-stick – om de installatiesoftware te draaien.

3. *Zet Ubuntu in het USB-installatieprogramma*
   Als je beide downloads binnen hebt, doe dan een lege USB-stick in de laptop en open de USB-installer. Selecteer de Linux Distribution van het dropdownmenu (Ubuntu), gebruik de Browse-knop om de Ubuntu-download op te zoeken en selecteer de USB Flashdrive-letter (de schijfletter waar de computer je USB-stick onder heeft geplaatst) en klik 'create'.



Als dit klaar is, verwijder je de USB-stick en sluit je de computer af.

Opstarten vanaf USB
Voordat je de USB kunt opstarten moet je je laptop vertellen dat hij dat moet doen. Dat kun je aangeven via een instelling in de BIOS. Je krijgt toegang tot het BIOS-menu als je de laptop opstart. Kijk van tevoren online welke toetsenbordcombinatie je moet indrukken om in het BIOS-menu te komen op jouw laptop. Dat verschilt namelijk per merk en type. Op veel machines komt er tijdens het opstarten een bericht dat aangeeft met welke toets(en) je in de setup komt ('entering setup' → press [key] to enter BIOS/setup/system configuration). Je kunt die instructie volgen. In de meeste gevallen is het de toets F1, F2, F3, F12 of DEL. Het is aan te raden om van tevoren uit te zoeken hoe je in de BIOS van jouw specifieke laptop de instructie om op te starten vanaf de USB-drive kunt instellen.

Doe de USB-stick in de laptop terwijl deze is uitgeschakeld. Vervolgens start je de laptop op en ga je naar het BIOS-menu. De instelling kan zijn ondergebracht in een menu-onderdeel zoals Startup → Boot of een menu-onderdeel zoals 'Boot', 'Boot options', of 'Boot selection menu'. Selecteer je USB-drive, of zorg ervoor dat je USB-drive bovenaan staan in de lijst van prioriteiten in de opstartvolgorde. Als een onderdeel van de lijst een '+' heeft, dan is er een submenu waar je de USB-vermelding waarschijnlijk kunt vinden. Meestal kun je de volgorde veranderen met de toetsen + en – van je numerieke toetsenbord. Navigeer vervolgens naar 'Exit' of 'Save and exit' en selecteer 'Exit saving changes' (of iets vergelijkbaars) zodat je voorkeur voor opstarten wordt bewaard/onthouden.

Dus:

- start de laptop op met de USB-stick ingeplugd
- ga naar het BIOS-menu
- kies ervoor om vanaf je USB-drive op te starten
- sla deze voorkeur op voordat je de BIOS verlaat

Ubuntu installeren
Nadat je de instelling om de laptop vanaf de USB-disk op te starten hebt opgeslagen en je de BIOS verlaat, moet het apparaat automatisch verder opstarten vanaf de USB-stick. Dat betekent dat het opstartmenu van het Ubuntu-installatieprogramma moet laden. Dit automatische installatieprogramma leidt je door de Ubuntu-setup.

Het kan zijn dat er tijdens het installatieproces om wifi-instellingen wordt gevraagd, maar daar hoef je verder geen aandacht aan te besteden, helemaal niet als je je wifikaart hebt verwijderd.

Selecteer bij 'Installatietype':

- vervang Windows door Ubuntu (al je Windows wilt verwijderen)
- versleutel de nieuwe Ubuntu-installatie om veiligheidsredenen
- gebruik LVM met de nieuwe Ubuntu-installatie

Kies een sterk wachtwoord (zie hoofdstuk 8 voor tips).

Het programma zal vragen om je naam te registreren, maar je hoeft hier niets in te vullen. Neem een computernaam en gebruikersnaam om in te loggen. Kies een sterk paswoord en vink aan zowel 'wachtwoord vereist om in te loggen' als 'encrypt de gebruikersmap/home folder'. Ubuntu voltooit daarna de installatie. Zodra Ubuntu is geïnstalleerd, zet je de laptop uit en verwijder je de USB-stick. Vervolgens kun je de laptop aanzetten zodat deze met Ubuntu opstart.

Als je verbinding met het internet maakt, ga dan naar de Ubuntu-icoon links bovenaan op je desktop en zoek naar updates. Accepteer en installeer alle beschikbare updates.

Ubuntu privacy-pimps

- Selecteer 'Systeeminstellingen' → 'Veiligheid en privacy' vanaf je desktop
- Bij 'Bestanden en applicaties/programma's' kun je bepalen welke informatie wordt bewaard over het gebruik van je bestanden en programma's.
- Bij 'Zoeken' kun je online zoekresultaten uitschakelen als je in de Dash zoekt. Dit schakelt Ubuntu's Amazon-integratie uit en voorkomt dat je Dash-zoekresultaten naar de Ubuntu- en Amazon-servers worden gestuurd. Als je met de rechtermuisknop op het Amazon-icoon op de desktop klikt, krijg je de optie 'losmaken van de launcher'. Hiermee verwijder je het van de desktop.
- Onder 'Diagnostieken' kunt je het versturen van foutmeldingen en incidentele systeeminformatie aan Canonical uitschakelen (opt-out).

Installatie Tails en extra informatie

Er zijn verschillende manieren om een USB-stick met Tails te maken:

1. Via een kloon van een USB-stick met Tails van een betrouwbare bron (dit is de aanbevolen methode – neem contact op met infosec@tcij.org voor hulp in het vinden van een gekloonde Tails-stick)
2. Handmatig met de Tails-installer (hiervoor heb je Ubuntu 15.10 of later nodig)
3. Handmatig via GNOME Disks (Ubuntu)
4. Handmatig via de Universal USB-installer (Windows)
5. Handmatig via commando (Mac, let op dit is de meest ingewikkelde methode)

Wij raden sterk aan om Tails te installeren via een gekloonde USB-stick. Handmatige installatie is niet even gemakkelijk en het lukt daarom niet altijd.

Installatietips

- Maak je USB-sticks klaar voordat je de installatie start. Tails heeft instructies over hoe je dat moet doen in Windows en Mac (installatiegidsen). Voor het maken van Ubuntu-sticks, zie hierna.
- Voor je eerste poging om op te starten met een Tails-stick (inclusief een extra Tails-stick als je handmatig installeert) moet je je laptop zo instellen dat deze van USB-stick opstart. Zie hierboven, 2.5, 'Opstarten vanaf USB'.
- We raden aan om Tails via de browser Firefox te downloaden. Firefox heeft namelijk een extensie beschikbaar voor 'Tails Download and Verify', die automatisch verifieert of je download de beoogde download is en dat er niet mee is geknoeid. De link en de instructies zitten in de Tails-installatie-instructies.

Instructies voor verschillende manieren om Tails te installeren vind je op de website van Tails: https://tails.boum.org/install/index.en.html

Noot: steeds meer gebruikers lukt het om de nieuwste versies van Tails op Mac-computers te gebruiken. Ontwikkelaars van Tails hebben echter minder ervaring in het gebruik van Mac en constateren verschillende problemen geconstateerd (bijvoorbeeld dat het niet lukt om wifi te gebruiken).

Opschonen en klaarmaken van een USB-stick voor Tails

Je hebt een USB-stick nodig van 4Gb of meer, bij voorkeur 16GB als je van plan bent om ook documenten op de stick op te slaan. Misschien gebruik je een stick die je al vaker hebt gebruikt of is het een stick waarop software staat voorgeïnstalleerd. Hoe dan ook, als je een stick gebruikt waar al informatie op staat/heeft gestaan, kun je de stick niet schoonmaken door alleen de bestanden in de prullenbak te gooien. Hierdoor zie je ze weliswaar niet meer in de bestandenlijst, maar ze worden niet echt verwijderd. Maar, voor je Tails-stick moet je beginnen met een volledig schone stick. We leggen hierna uit hoe je de stick helemaal opschoont. Verder moeten er een paar instellingen op de USB-stick worden aangepast, als voorbereiding om de laptop met de stick op te kunnen starten met Tails.

1. Installeer GParted → ga naar het dashboard van de Ubuntu Software op je laptop en zoek naar 'GParted'. Kies installeren.
2. Doe je USB-stick in de laptop.
3. Open GParted. Ga naar GParted → Refresh Devices
4. Je USB moet als drive worden getoond rechts bovenaan in het dropdownmenu (in de lijst vermeld als as /dev/sdb or dev/sdc). Er wordt ook getoond hoeveel ruimte er beschikbaar is op je USB-stick. Selecteer deze drive.
5. Je ziet nu een lange rechthoek bovenaan het scherm met groene uitlijning, misschien met ruimte aan de linkerkant of een rechthoek met gele schaduw. Klik met je rechtermuisknop en selecteer 'verwijderen (unmount)', klik nogmaals met de rechtermuis en selecteer 'delete'.
6. De kleuren in de rechthoek zijn nu verdwenen en vervangen door grijs. Klik op de rechthoek en selecteer 'Nieuw'.
7. Er verschijnt een scherm getiteld 'maak een nieuwe partitie'. Bij 'File System' selecteer je 'fat32', en bij 'Label' typ je 'TAILS'. Klik vervolgens 'Add'. *fat32 = File Allocation Table 32 bits*
8. Klik op het groene spinnetje (net onder de optie 'Partitie' in de toolbar bovenaan in het scherm)
9. Er verschijnt een pop-up. Selecteer 'Apply' om wijzigingen aan het apparaat door te voeren en kies 'Sluiten' als het bericht 'alle wijzigingen zijn succesvol uitgevoerd' verschijnt.
10. Klik nu met de rechtermuisknop op de lange groene rechthoek en kies 'Manage Flags' → selecteer 'opstarten, en zet de laptop uit. Hiermee weet de laptop dat er een drive is die als opstartsysteem voor de computer kan worden gebruikt.

Je kunt de USB-stick nu veilig verwijderen. Hij is schoon en klaar voor Tails.

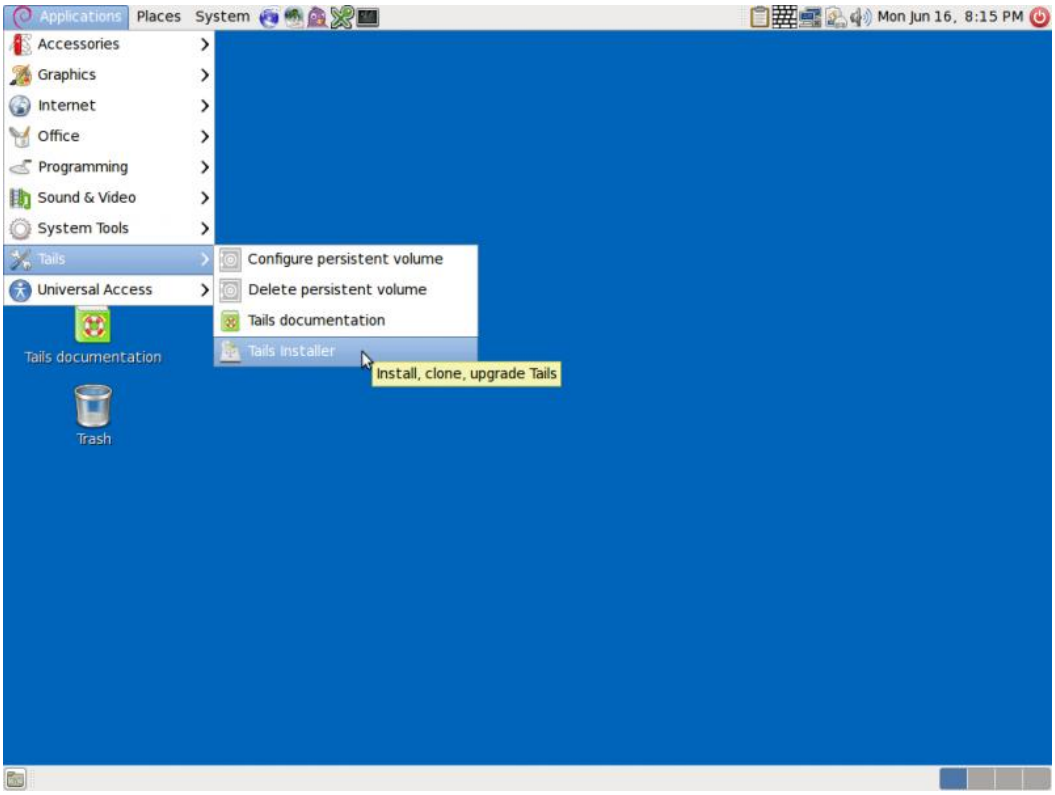
Het klonen van een USB-stick met Tails

Als je een gekloonde Tails-stick hebt, hoef je alleen je laptop zo in te stellen dat deze vanaf de USB-drive opstart (zie hiervoor, opstarten vanaf USB). Je kunt vervolgens de Tails-stick in de laptop doen en de laptop opstarten.

Als je Tails op een nieuwe USB-stick wilt klonen, bijvoorbeeld door een kloon te maken van een stick van een vriend, of als je je eigen Tails-stick wilt klonen voor een collega, volg dan deze stappen.

Maak eerst een nieuwe, schone USB-stick met Gparted om Tails op te zetten. Vervolgens:

1. Start het Tails-systeem met de huidige Tails-stick
2. Doe de schone USB-stick in een van de USB-poorten
3. Ga op de Tails-desktop naar Applications → Tails → Tails Installer



4. Er opent zich een nieuw venster. Selecteer hier ‘Install by cloning’ (installeren door te klonen)

5. Het Tails-installatievenster toont de schone USB-stick bij ‘Target Device’. Klik ‘Install Tails’ onderaan het venster en klik ‘Yes’ in het pop-upscherm om te bevestigen. Nu wordt de kloon of je Tails-installatie gemaakt op de schone USB-drive.

Als de kloon klaar is, zegt de Tails-installer: Installation complete! (installatie voltooid)

6. Als de installatie is voltooid sluit je je systeem af en probeer je deze te herstarten vanaf de nieuwe drive om te controleren of het goed werkt.

Upgraden van Tails

Het Tails-systeem zoekt automatisch naar updates en downloadt deze. Het is belangrijk om het systeem up-to-date te houden. Als je Tails opstart en verbindt met Tor krijg je automatisch een dialoogvenster als er een upgrade beschikbaar is, met de suggestie het systeem te upgraden.

Het kan overigens soms een tijdje duren voordat Tails met het internet is verbonden na het opstarten. Hierdoor is het niet altijd mogelijk om de controle op upgrades tijdens het opstarten te doen. Je kunt ook handmatig controleren of er upgrades zijn. Dat doe je door de Terminal te openen (het icoon met het zwarte vierkant in de bovenste toolbar van de Tails-desktop) en het volgende commando te typen: `tails-upgrade-frontend-wrapper`

Vervolgens klik je enter. Tails controleert nu of er updates zijn en vertelt je of je systeem up-to-date is of niet.

Meer informatie over het upgraden van Tails en probleemoplossing als Tails niet automatisch upgrades voorstelt, kun je vinden op de Tails-website: https://tails.boum.org/doc/first_steps/upgrade/index.en.html

Het gebruik van Tails

Voordat je Tails kunt gebruiken, moet je eerst je laptop vertellen dat deze vanaf de USB-drive moet opstarten, zie Opstarten vanaf USB. Als je met Tails opstart krijg je een scherm in beeld met de opties 'Live' en "Live failsafe'. Gebruik de pijltjestoetsen om 'Live' te selecteren en klik op enter. Vervolgens krijg je de keuze 'More options'. Het is niet nodig om dit menu te gebruiken tenzij je Tails zo moet instellen dat je Tor-censuur kunt omzeilen. Als dat niet zo is, selecteer je 'no', 'Login' en vervolgens kun je Tails verkennen.

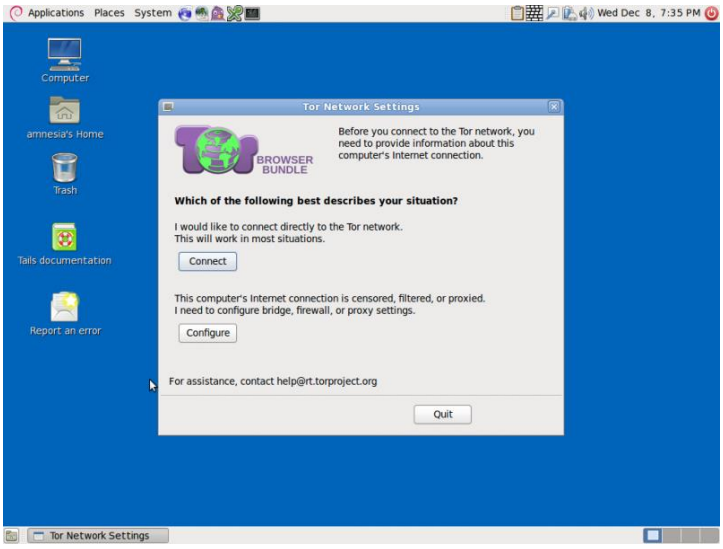
Als je 'ja' kiest en dus 'More options' selecteer, krijg je de volgende onderdelen te zien:

- '*Administrative password*'. Het is onwaarschijnlijk dat je een administratief wachtwoord wilt aanmaken, tenzij je toegang wilt tot de interne harde schrijf van de computer (dat raden we af omdat het tot onnodige veiligheidsrisico's kan leiden).
- '*Spoof all MAC addresses*'. Deze moet automatisch geselecteerd zijn. Het is een goede mogelijkheid om de serienummers van je netwerkkaarten te verbergen en dit helpt dus om je locatie verborgen te houden.
- *'Network configuration'*. Hier heb je twee opties: direct verbinding maken met het Tor-netwerk of het configureren van een bridge in geval van censuur ('*This computer's internet connection is censored, filtered or proxied. You need to configure bridge, firewall or proxy settings*'). Als je netwerk geen Tor-verbindingen toestaat, selecteer je de laatste.
- *'Disable all networking'*. Als je offline wilt blijven.

Het gebruik van Tails via bridges (omzeilen van censuur)

Toelichting: bridges helpen je om toch connectie te maken met het Tor-netwerk in situaties waarin het niet wordt toegestaan om met het Tor-netwerk te verbinden. Bridges zijn Tor-relays (zogenaamde nodes of computerpunten) die verkeer van het Tor-netwerk ontvangen en doorgeven om censuur te omzeilen.

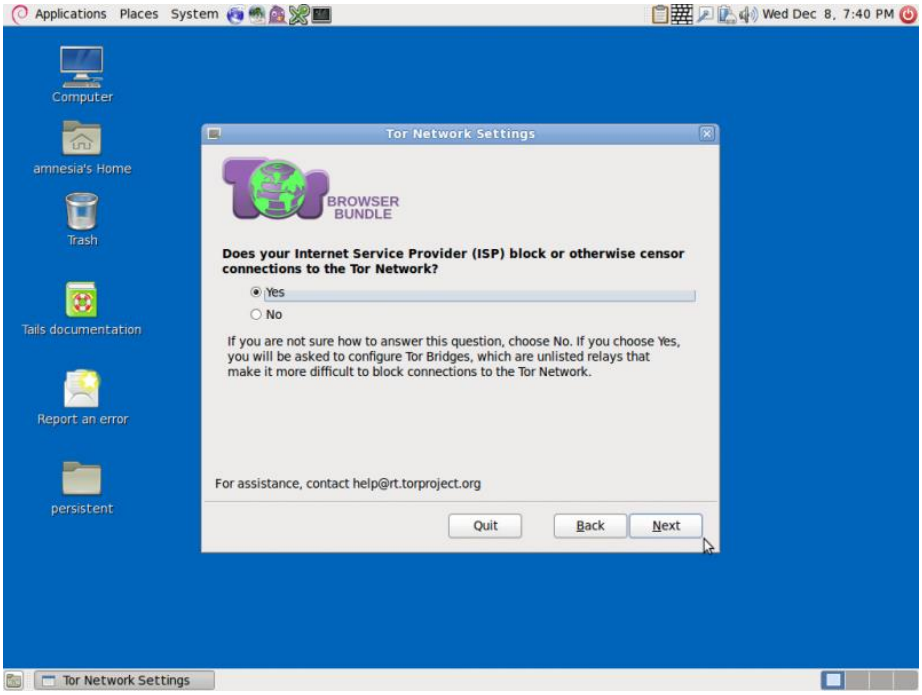
Om bridges te gebruiken, volg je een iets andere opstartprocedure. Als je opstart met de Tails-stick en je kunt kiezen voor 'More options?', selecteer dan 'Yes' om door te gaan. Bij *'Network configuration'*, selecteer je *'This computer's internet connection is censored, filtered of proxied. You need to configure bridge, firewall or proxy settings'*.



Als je vervolgens verbinding met het internet zoekt, komt de Tor-browser met een venster waarin dezelfde vraag wordt gesteld.

Als de toegang wordt geblokkeerd, kies je voor 'Configure'. Vervolgens krijg je de vraag of je ISP connectie met het Tor-netwerk blokkeert of censureert. Kies hier voor 'yes' als dat het geval is om bridges te

configureren. Vervolgens klik je op ‘next’.



Je krijgt nu een venster waarmee je een of meer ‘bridges’ – (series van nummers die een Tor-relay identificeren) opent. Voor het verkrijgen van bridges, ga je naar https://bridges.torproject.org, of als dat niet lukt, stuur een e-mail naar bridges@torproject.org via een gmail.com of yahoo.com e-mailadres, met de tekst ‘get bridges’ in de body van het bericht en je krijgt bericht terug met een link bridges.

Het gebruiken van een bridge kan extreem traag zijn, maar het werkt goed als je censuur moet omzeilen.

Een persistent volume (opslagruimte) op je Tails-stick maken
Voor het maken van een persistent volume binnen Tails ga je naar Applications → Tails → Configure persistent volume. Als je een zeer sterk wachtwoord (zie hoofdstuk 8) heb ingevoerd, kun je kiezen wat voor soort bestanden je wilt opslaan op het volume. Selecteer hier ‘all types’ om je opties open te houden.

Vanaf nu krijg je iedere keer dat je de laptop opstart vanaf de Tails-stick twee vragen: ‘Use persistence?’ en ‘More options?’ (zoals eerder). Als je je klikt op ‘use persistence’ en het wachtwoord invult, dan krijg je toegang tot alle data die je op het persistent volume hebt bewaard in voorgaande sessies (zoals de geconfigureerde e-mailclient, IM-client, wachtwoordmanager en bestanden).

E-mail in Tails

Lees eerst hoofdstuk 5 over e-mail voordat je verder leest in dit hoofdstuk. Bekijk ook de documentatie van Tails over Icedove (Thunderbird) op https://tails.boum.org/doc/anonymous_internet/icedove/index.en.html .*

Tails bevat een voorgeïnstalleerde e-mailclient genaamd Icedove. Dit is een heruitgave van Thunderbird, zoals gedocumenteerd in hoofdstuk 5. Daarnaast is Enigmail voorgeïnstalleerd, een

extensie voor Icedove die encryptie van e-mail ondersteunt. Als je al met Thunderbird/Enigmail werkt om je e-mails te versleutelen op je computer, dan zou je geen problemen moeten ondervinden in het werken met Icedove via Tails. De instructies van hoofdstuk 5 zijn ook hier van toepassing.

Je sleutel importeren van een laptop/besturingssysteem
Veel mensen gebruiken verschillende Tails-sticks, e-mailadressen, PGP-sleutels, etc. voor verschillende projecten. Dat is een prima manier om veilig te werken en je activiteiten op te splitsen. Maar het kan zijn dat je een encryptiesleutel wilt gebruiken binnen Tails die je op een andere computer of laptop hebt aangemaakt. Je hebt hier een reserve-USB-stick voor nodig. Houd er wel rekening mee dat dit je anonimiteit binnen Tails kan opheffen.

Doe de USB-stick in de laptop waarop de encryptiesleutel staat die je naar de nieuwe plek wilt verplaatsen. Open Thunderbird en ga naar Enigmail → Key management. Zoek je e-mailadres en sleutel in je contactenlijst en klik met je rechtermuisknop om het te selecteren. Vervolgens kies je 'Export keys to file' → 'Export secret keys'. Zoek je USB-drive en selecteer deze als locatie waar je je sleutel wilt opslaan. Verwijder de USB-stick vervolgens en start je Tails-systeem op. Zodra Tails is opgestart en met het internet is verbonden, doe je de USB-stick met de opgeslagen sleutel in je laptop. Klik op Tails' OpenPGP encryption applet (het icoontje met klembord bovenaan rechts van het navigatiemenu) en selecteer → Manage keys → File → Import. Open de bestandenlijst van je USB-stick om de sleutel op te zoeken en selecteer 'Import'.

Als je de sleutel in Tails hebt geïmporteerd is het verstandig om de sleutel op een veilige manier (dus niet alleen deleten, zie ook hoofdstuk 4, data veilig delen) van de USB-stick te verwijderen. Het is namelijk niet verstandig om je geheime sleutel bij je te dragen op een onbeveiligde USB-stick. Gebruik hiervoor de 'Wipe'-functie van Tails (klik met je rechtermuisknop op het bestand met de sleutel op de USB-stick). Hiermee kun je het bestand veilig en volledig verwijderen.

OpenPGP Encryption Applet
Omdat alle internetverbindingen van Tails via het Tor-netwerk lopen, loopt de verbinding met je e-mailprovider ook via Tor. Gebruikers van sommige e-mailproviders kunnen problemen hebben met het configureren van hun e-mailaccounts op Icedove via Tails, omdat de Tails de connectie wil omleiden naar het Tor-netwerk om je locatie te verbergen.

Tails heeft voor die situatie een alternatieve manier om encryptie in e-mail en e-mailbijlagen te gebruiken. In plaats van een e-mailclient te gebruiken om het hele e-mailbericht te versleutelen, kun je de betreffende tekst selecteren en encrypten naar de sleutel van de gewenste ontvanger vóórdat je die (versleutelde) tekst in een e-mail plakt (als je de e-mail in de webbrowser opstelt).

Importeren van de openbare sleutel (public key) van je contactpersoon
Na naar de OpenPGP-encryptie-applicatie (het icoontje met klembord, rechtsboven in je navigatiemenu) → Manage keys → en kies of een van de twee mogelijkheden:

- Remote → zoek remote keys (als je de sleutel van de contactpersoon nog niet hebt). Voer de naam van de contactpersoon in en klik op 'zoeken'
- File →Importeren (als je de sleutel al in een bestand hebt opgeslagen).

Versleutelen van de tekst
Typ je bericht in de Gedit Text Editor. Je vindt deze bij Applications (linksboven in het navigatiemenu) → Accessories → gedit Text Editor. Vervolgens selecteer je de getypte tekst (Ctrl + A) en kopieer je

deze naar het klembord (Ctrl + C of rechtermuisknop/kopieer). Ga naar de OpenPGP encryptie-applicatie, kies → Sign/encrypt Clipboard with Public Keys → selecteer de ontvanger van je e-mail (je moet de sleutel van deze persoon al hebben geïmporteerd), onderteken het bericht met het e-mailadres dat je gebruikt om de mail te versturen en klik OK. Plak vervolgens de tekst in het e-mailbericht (Ctrl + V) dat je aan het opstellen bent en verstuur deze.

Let erop dat je het bericht hebt versleuteld, zodat alleen de beoogde ontvanger deze kan lezen. Dat betekent ook dat je heb bericht zelf niet meer kunt lezen of ontsleutelen zodra je het heb versleuteld. Daarom is het verstandig om ook je eigen publieke sleutel bij de encryptie toe te voegen als je deze methode gebruikt. Je kunt het dan zelf ook ontsleutelen als je je verzonden berichten wilt teruglezen.

De tekst ontsleutelen/decrypten

Om de tekst te ontsleutelen, selecteer je de betreffende tekst. Voeg de tekst "-----BEGIN PGP MESSAGE-----" en "-----END PGP MESSAGE-----" toe en plak de tekst naar het klembord (Ctrl + C of rechtermuisklik/copy). De OpenPGP-applicatie (icoon met klembord) laat nu een sleuteltje zien: dat betekent dat het versleutelde tekst bevat. Als de tekst alleen is ondertekend maar niet versleuteld zie je hier een zegel. Dat betekent dat het klembord alleen ondertekende tekst bevat. We gaan ervan uit dat je een sleuteltje ziet: klik op de OpenPGP-applicatie (icoontje met klembord) en selecteer 'Decrypt/Verify Clipboard' van het menu. De ontsleutelde tekst wordt nu getoond in het venster Output van GnuPG.

E-mailbijlagen versleutelen

Het is gemakkelijk om bestanden te versleutelen met openbare sleutels en deze als e-mailbijlage te versturen via Tails. Klik met je rechtermuisknop op het betreffende bestand, kies → Encrypt → vul het e-mailadres van de ontvanger in (onderteken het bericht als het adres waarmee je de e-mail gaat versturen) en klik op OK. Je ziet nu een duplicaat van het geselecteerde bestand met de extensie '.pgp'. Dit betekent dat het bestand is versleuteld. Voeg het .pgp-bestand aan je e-mail toe. Vervolgens kan deze alleen worden geopend en ontsleuteld door de gekozen ontvanger.

Hoofdstuk 3: veilig browsen

Risico's tijdens het surfen op het web:

- verzamelen van je identiteitsgegevens
- verzamelen van je surfgedrag, inclusief de pagina's die je bezoekt en wanneer
- verzamelen van je wachtwoorden en automatisch voor-ingevulde informatie
- verzamelen van je locatie (en vorige locaties)
- malware-injectie (toevoegen van kwaadaardige software, soms spyware)
- blokkeren van toegang tot bepaalde websites
- blokkeren van mogelijkheid tot gebruik van anonieme browsers

Tips voor informatiebeveiliging tijden het surfen:

- voor je dagelijkse activiteiten gebruik je een algemene browser, met extensies/plug-ins voor extra privacy-beveiliging
- wil je censuur/blokkades tegengaan en je echte locatie te verbergen, surf dan anoniem via de Tor-browser

Een webbrowser is een softwareapplicatie die je gebruikt om te kunnen surfen op het World Wide Web, oftewel 'het internet', een venster naar de wereld.

Vanwege de enorme mogelijkheden in websurfen brengen sommige overheden beperkingen aan in toegang tot bepaalde websites. Dit belemmert de vrijheid van mensen in hun surfmogelijkheden en natuurlijk stelt dit lokale journalisten, onderzoekers en buitenlandse correspondenten voor problemen. Ook al kent de toegang tot het internet in het westen nauwelijks restricties, we hebben wel serieuze privacy-problemen tijdens het websurfen. Het feit is dat de meeste serviceproviders en websites enorme hoeveelheden data van hun klanten/bezoekers verzamelen. De Britse overheid heeft eind 2016 wetgeving aangenomen die internetproviders verplicht om iedere internetconnectie van ieder individu inclusief locatiedata en identificatienummer van het verbonden apparaat te registreren. Ook alle zoekacties in de browsers worden vastgelegd.

In dit hoofdstuk worden een aantal opties aangedragen die helpen om de inbreuk op je privacy tijdens het surfen te minimaliseren in verschillende situaties.

Welke browser moet je gebruiken

Veel mensen zijn zich onbewust van de privacy-problemen van webbrowsers. Ze gebruiken de browser die al op het systeem is voorgeprogrammeerd. Er zijn echter alternatieven die veiliger zijn in gebruik en waarvan je de functionaliteit nog verder kunt verbeteren via uitbreidingen (het toevoegen van extensies, zogenaamde plug-ins).

Er zijn vele browsers die gespecialiseerd zijn voor bepaald gebruik. Wij bevelen drie opensource-browsers specifiek aan:

- Firefox als webbrowser voor algemeen gebruik op Linux- en Windows-computers;
- Chromium als webbrowser voor Mac-computers;
- Tor als webbrowser die je locatie en identiteit anonimiseert en webcensuur voorkomt (geschikt voor Linux, Windows en Mac).

Toelichting: we raden Firefox aan voor Linux en Windows, maar niet voor Mac, omdat Firefox conflicten kan geven met de Tor-browser op een Mac (aangezien Firefox en Tor op dezelfde code zijn gebaseerd).

Browsers voor algemeen gebruik
Met algemeen gebruik wordt hier bedoeld: je dagelijkse surfactiviteiten zoals bezoek aan websites die normaal gesproken geen restricties hebben en sites waarop je inlogt, zoals platforms voor sociale media, LinkedIn, websites van kranten, YouTube, webshops, etc.

- Firefox is een populaire opensource-webbrowser. Gebruik je Windows, dan moet je Firefox voor jouw versie van het besturingssysteem en taal downloaden via www.getfirefox.com.
  Gebruik je Linux/Ubuntu dan hoort Firefox al te zijn geïnstalleerd.
- Chromium is een opensource-kloon van Google Chrome. Je kunt Chromium voor de Mac downloaden via https://www.macupdate.com/app/mac/36244/chromium
  (alternatief: ga naar https://www.macupdate.com en zoek 'Chromium').

Extensies voor verhoging privacy
Als je een algemene webbrowser gebruikt, kun je er zeker van zijn dat je identiteit, locatie en surfactiviteiten worden geregistreerd. Er is echter een aantal extensies die je kunt installeren om je privacy en veiligheid enigszins te verbeteren. Je kunt een keur aan privacy-verhogende extensies vinden via https://addons.mozilla.org/en-US/firefox/extensions/privacy-security/, die geschikt zijn voor zowel Firefox als Chromium.

We raden in het bijzonder aan om de volgende opensource-extensies te installeren:

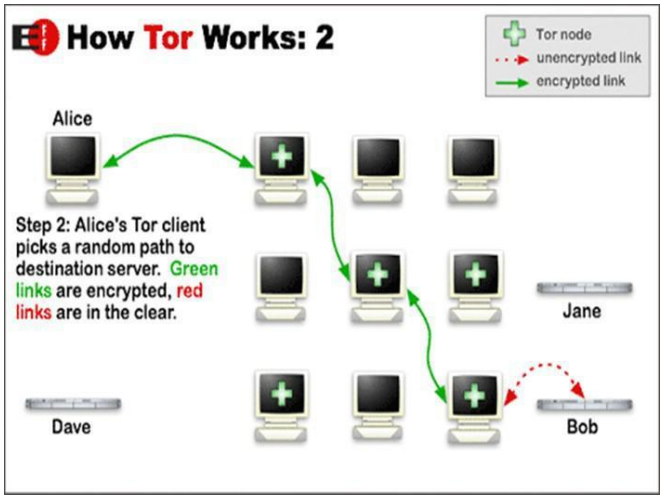
- HTTPS Everywhere: forceert encryptie voor alle verbindingen tussen webbrowser en webserver die je bezoekt. Link: https://www.eff.org/https-everywhere

- NoScript: blokkeert JavaScript. JavaScript is een essentieel onderdeel op verschillende websites, maar de software kan worden misbruikt om je surfgedrag te volgen, je wachtwoorden te lekken en om malware toe te voegen. NoScript is heel effectief, maar daarvoor moet je websites rechten toekennen of weigeren, afhankelijk van in hoeverre je de site vertrouwt. Link: https://noscript.net/

- Ghostery: blokkeert een flinke lijst trackers die je surfgedrag volgen en die in Ghostery-database zijn opgenomen. Let er wel op dat je 'Ghostrank' uitschakelt bij 'Instellingen' → 'Opties' omdat Ghostery zelf je data gebruikt voor marketingdoeleinden. Link: https://ghostery.com

- LastPass: een wachtwoordgenerator en –manager voor Firefox. Link: https://lastpass.com/

Browser voor anoniem surfen: Tor



https://www.torproject.org/

Over Tor

De Tor-browser is speciaal ontworpen voor anonimiteit tijden het surfen. Dat gebeurt door het routen van al het internetverkeer via het Tor-netwerk. Tor staat voor 'The Onion Router. Deze browser verhindert dat internetproviders accurate informatie kunnen opslaan over je surfgeschiedenis.

Dat werkt als volgt: het Tor-netwerk is een wereldwijd netwerk van computers die Tor-nodes worden genoemd. Die hebben verbindingen met encryptie met elkaar. Als de Tor-browser wordt opgestart, zoekt deze verbinding met een van de nodes. Die maakt vervolgens verbinding met een tweede, die op zijn beurt met een derde. Die nodes kunnen zich overal ter wereld bevinden en de eerste en de derde kunnen elkaar niet zien/achterhalen. De derde node maakt connectie met het internet en haalt de webpagina's van de sites die je bezoekt. Die websites kunnen niet zien waar je bent of wie je bent, dat wil zeggen: zolang je je niet identificeert door in te loggen op diensten die met je werkelijke identiteit kunnen worden geassocieerd.

De Tor-browser is trager dan een gewone browser omdat al het verkeer via verschillende plekken in de wereld wordt gestuurd. Een prijs die je graag moet willen betalen om zo je anonimiteit te waarborgen.

Om er zeker van te zijn dat je veilig kunt surfen, schakelt Tor automatisch HTTPS-Everywhere in. Extensies als Flash, RealPlayer en QuickTime worden automatisch uitgeschakeld. Maar je kunt de instellingen aanpassen om de gebruikersvriendelijkheid naar je eigen voorkeuren in stellen.

Beperkingen/blokkades omzeilen

Als de netwerkprovider die je gebruikt de toegang tot het Tor-netwerk blokkeert (dat kan een netwerk van een universiteit zijn of misschien een volledig land), kun je zogenaamde 'bridges' (bruggen) gebruiken om alsnog toegang te krijgen.

Bridges zijn privé Tor-relays (nodes voor computertoegangspunten die verkeer ontvangen op het Tor-netwerk en deze doorgeven) waarvan het minder waarschijnlijk is dat ze worden geblokt en die dus helpen om de censuur te omzeilen.

Zo gebruik je een bridge: start de Tor-browser. Klik op de groene ui (links van de adresbalk) en klik op Tor Network Settings → 'My ISP blocks connections to the Tor network' ("mijn ISP blokkeert connecties via het Tor-netwerk").

Via het vak dat verschijnt, kun je een of meerdere bruggen binnengaan (serie van nummers die een Tor-relay kunnen identificeren). Om de bridges te kunnen gebruiken, ga naar https://bridges.torproject.org. Als je die website niet kunt benaderen, stuur dan een e-mail naar bridges@torproject.org, via een gmail- of yahoo.com-adres met de tekst 'get bridges' in de body van het bericht en je zou een link naar bridges teruggestuurd moeten krijgen. Het gebruik van een

brug kan een extreem traag zijn in het maken van internetverbinding, maar het werkt wel en is dus een prima optie als je censuur moet omzeilen.

Anoniem blijven

De Tor-browser heeft een beveiligingsscherm waarin de gebruiker de gewenste beveiligingsopties kunnen instellen. In de Tor-browser klik je op de groene uit (links van de adresbalk) en selecteer 'Privacy and Security Settings' om het scherm en de verschillende opties te bekijken. Het scherm is standard op 'laag' ingesteld omdat dit de gebruikersvriendelijkheid verhoogt. Zet de beveiliging op het hoogste niveau als je Tor op het hoogste veiligheidsniveau wilt gebruiken, of als je volledig anoniem wilt surfen.

Open geen documenten zoals doc, docx of PDF zolang je nog online ben via de Tor-browser. Deze document-formats kunnen onderdelen bevatten die onafhankelijk connectie met het internet zoeken. Je loopt op die manier alsnog kans dat je IP-adres wordt onthuld. Verzeker jezelf ervan dat je offline ben of een andere computer gebruikt als je met zulke documenten werkt.

Draai geen BitTorrent via Tor omdat dit je IP-adres kan onthullen en in verhouding veel capaciteit van het Tor-netwerk gebruikt.

Verzeker je er steeds van dat je nog met de nieuwste versie van de Tor-browser werkt. Je krijgt een updatebericht op de homepage van de Tor-browser als er een update beschikbaar is. Je kunt ook controleren of je met de laatste versie werkt door op de groen uit in de browser te klikken (links naast de adresbalk) en te kiezen voor 'Check for Tor Browser update'.

Het installeren van Tor

Mac, Windows
We raden sterk aan om Tails te starten via een gekloonde USB-stick (handmatige installatie is niet even eenvoudig en lukt daarom niet altijd).

Linux/Ubuntu

1. Download de Tor-browser voor via https://www.torproject.org/, selecteer 'Save file' en wacht tot de download is voltooid.

2. Ga in je bestandenlijst naar de downloads (of de map waar je je downloads laat opslaan) en klik met de rechtermuisknop op het bestand. Selecteer 'Extract here', open het uitgepakte bestand (bijvoorbeeld tor-browser_en-US), en klik 'Tor browser setup'.

3. Je kunt nu kiezen of je wilt verbinden of configureren. Tenzij je netwerkprovider de toegang tot het Tor-netwerk blokkeert, kun je hier 'Connect' kiezen. Als je netwerkprovider de toegang blokkeert, lees dan het onderdeel hiervoor: 'Beperkingen/blokkades omzeilen'.

4. De Tor-browser zou nu moeten opstarten. Je moet nu een icoon 'Tor browser' in je bestandenlijst zien: dit is het opstart-icoon van het programma. Je kunt deze naar je desktop slepen of in de taakbalk vastzetten zodat je de browser snel kunt gebruiken.

Hoofdstuk 4: omgaan met data

In dit hoofdstuk leer je hoe je op een veilige manier met je data kunt omgaan.

Risico's:

- verlies
- corrupt/onbetrouwbaar/defect
- interceptie
- diefstal
- herstelmogelijkheden 'verwijderde' data
- anonimiseren ongedaan maken/compromitteren van metadata

Acties voor informatiebeveiliging:

- back-up van data
- versleutelen van data
- op een veilige manier delen van bestanden
- op een veilige manier bestanden/data verwijderen
- metadata verwijderen

Je moet met verschillende risico's rekening houden als je data opslaat of meeneemt. Je data kan worden onderschept, gestolen, je kunt data verliezen en de data kan corrupt raken. Het verschil tussen onderscheppen en diefstal is dat je als eigenaar onderschepping meestal niet merkt, maar diefstal wel. Onderschepping betekent dat er in het geheim een kopie is gemaakt, terwijl diefstal betekent dat het opslagapparaat fysiek is weggenomen (dus de laptop, USB-stick of harddisk met de data). Dat laatste merk je uiteraard, terwijl onderschepping misschien onontdekt blijft.

Als gevoelige data in de handen komt van je tegenstander, kan dit ernstige gevolgen voor de journalist en/of zijn bron met zich meebrengen. Het is dus verstandig je digitale bestanden te beveiligen. Je kunt je digitale bestanden op verschillende manieren beveiligen. Je kunt het bijvoorbeeld eenvoudigweg opslaan op een klein opslagapparaat (USB-drive, geheugenkaart of externe harddisk) en die zo goed mogelijk verbergen. Dat kan in bepaalde gevallen effectief zijn, maar de volledige veiligheid van de data is er in dat scenario ervan afhankelijk of het apparaat onontdekt blijft.

Om je data te beschermen tegen ongeautoriseerde toegang is het belangrijk om de data te versleutelen. Dat kun je bijvoorbeeld doen met VeraCrypt. Dit is een eenvoudig programma waarmee je bestanden of volledige schijven kunt versleutelen en zelfs het bestaan ervan kunt verbergen.

VeraCrypt voor versleuteling

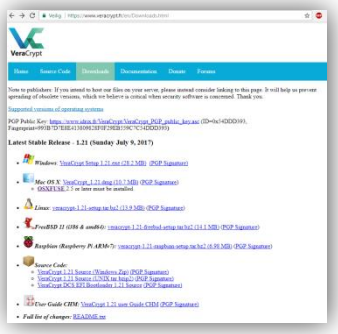
VeraCrypt is opensource-software voor het versleutelen van bestanden
Download: https://www.veracrypt.fr/en/Downloads.html
(Mac-gebruikers moeten ook FUSE voor macOS downloaden: https://osxfuse.github.io/)

Hier vind je goede, begrijpelijke documentatie over VeraCrypt:
https://www.veracrypt.fr/en/Documentation.html

Met VeraCrypt kun je een versleutelde container maken die als een soort digitale kluis voor bestanden werkt, beveiligd met een wachtwoord. Als de kluis is gemaakt en er zijn bestanden in opgeslagen, kun je deze naar een extern opslagapparaat verplaatsen, bijvoorbeeld een USB-drive, of je verstuurt de kluis via het internet naar anderen. Zelfs als het bestand wordt onderschept kan niemand in de digitale kluis kijken, zodat de inhoud ervan veilig blijft. De inhoud is alleen toegankelijk voor degenen met het wachtwoord.

*Belangrijk! Vergeet je wachtwoord niet, want er is geen enkele manier om de data terug te krijgen als het bestand is versleuteld. Verlies van wachtwoord betekent verlies van data.**

Installatie van VeraCrypt/Fuse



Download VeraCrypt en installeer deze op je apparaat. De installatie werkt op dezelfde manier als die van andere programma's. VeraCrypt werkt op dezelfde manier in Windows, Mac en Linux-systemen. De versleutelde containers zijn bovendien onderling compatibel op die systemen. Dat helpt je om veilig met andere mensen samen te werken, omdat je niet hoeft te weten met welk besturingssysteem iemand werkt. Hier vind je een uitgebreide tutorial voor VeraCrypt. Mac-gebruikers moeten naast Veracrypt ook FUSE for macOS downloaden.

Een bestand versleutelen met VeraCrypt

Stap 1 – maak een versleuteld volume

Om een volume met encryptie te maken, start je VeraCrypt. Je maakt van tevoren een leeg bestand aan op de plek die als container gaat fungeren (bijvoorbeeld een leeg kladblok-bestand). Vervolgens:

- Op harde schijf: selecteer 'Volumes' → 'Create New Volume' (creëer nieuw volume) → 'Create an encrypted file container' (maak een versleutelde container voor bestanden) -> selecteer 'Standard VeraCrypt volume'-> en selecteer het bestand waarin de container op je computer moet worden opgeslagen. Kies 'ja' als om overschrijven wordt gevraagd. Je kunt het bestand later verplaatsen. Geef de container een onopvallende naam.

  Op een USB-stick of externe harde schijf: selecteer 'Volumes' → Create New Volume' → Encrypt a non-system partition/drive' (versleutel een externe partitie of drive). Bij 'Volume Location' kies je 'Select device'. Tip: om de USB-drive te ontsleutelen heb je VeraCrypt ook nodig, dus als je van plan bent om bestanden te ontsleutelen op een computer waarop VeraCrypt niet is geïnstalleerd, zet dan ook het installatiebestand van VeraCrypt op de USB-stick, naast de versleutelde container.

- Het volgende venster is getiteld 'Encryption Options' (versleutelingsopties). De standaard-instellingen volstaan.

- Daarna zie je het scherm 'Volume size'. Selecteer hier de grootte van de container. De grootte bepaalt hoeveel data je in de container kunt opslaan. Je losse bestand mag niet groter zijn dan 4 GB (in verband met de formatmogelijkheden, zie hieronder).

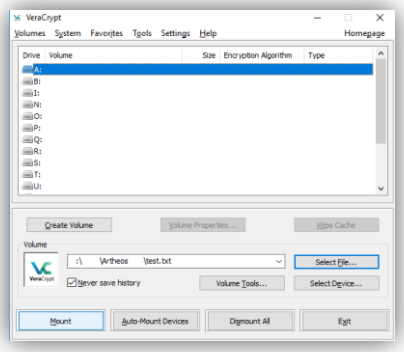
- Vervolgens word je gevraagd het wachtwoord voor het volume in te stellen. Kies een veilig wachtwoord (zie hoofdstuk 8) en … vergeet deze niet!!!

- Het volgende venster is getiteld 'Format Options'. Selecteer 'FAT'.

- Het programma gaat nu het volume versleutelen. Maak een paar willekeurige muisbewegingen – daarmee kan de computer een betere encryptiesleutel aanmaken – voordat je op 'Format' (formatteren) klikt. Vervolgens wordt het volume aangemaakt. Afhankelijk van de grootte, het gekozen encryptie-algoritme en de snelheid van je computer duurt het aanmaken een paar seconden of wat langer.

- Als het volume is aangemaakt, klik dan op 'Exit' om naar het hoofdscherm van het programma terug te keren.

Gefeliciteerd – je hebt nu een veilig volume aangemaakt.



Stap 2 – Te versleutelen bestanden in het volume met encryptie plaatsen
Nu kun je het volume openen en daar bestanden in plaatsen. Binnen VeraCrypt kies je een Drive en vervolgens ga je naar 'Select File' (selecteer bestand) → zoek het bestand dat je als container hebt aangemaakt en selecteer deze, kies vervolgens 'Mount' (activeren). Voer het wachtwoord in en klik op OK. De VeraCrypt-container verschijnt nu op je systeem als een aparte drive (op dezelfde wijze als je C-schijf, een USB-stick of een externe harde schijf). Je kunt nu bestanden in de container plaatsen op dezelfde manier zoals je dat met een USB-stick zou doen. Ga naar Mijn Computer of de Finder (Mac), selecteer de gewenste bestanden en sleep ze naar de container.

Als je de bestanden in de container hebt geplaatst, kun je de container sluiten door te klikken op 'Dismount' in VeraCrypt. De container ziet er nu uit als een willekeurig bestand op je computer.

Verborgen volumes met encryptie

Binnen het VeraCrypt-volume kun je een verborgen volume aanmaken. Verborgen, versleutelde volumes zijn volumes die binnen het normale VeraCrypt-volume niet zomaar te zien zijn. Hiermee creëer je extra veiligheid als je gedwongen bent het wachtwoord te verstrekken. Je zet dan wat bestanden in het normale volume als afleiding. In het verborgen volume zet je de gevoelige informatie.

Eerst geef je het normale VeraCrypt-volume, zoals hierboven beschreven, een wachtwoord. Dit is als het ware de buitenste schil. Deze container is zichtbaar in je bestandenlijst als een willekeurig bestand. In deze container kun je verschillende gevoelige bestanden die je wilt versleutelen en geheim wilt houden. Je kunt het ook gebruiken als afleiding, voor het geval een tegenstander je dwingt om het wachtwoord te geven. Met een verborgen volume binnen VeraCrypt ben je hierop voorbereid.

Niemand kan het verborgen volume binnen je VeraCrypt-container zien. Voor zover bekend is, kan het bestaan van dit verborgen volume niet worden aangetoond, ook niet met het meest verfijnde onderzoek. Niemand kan het volume zien en alleen de maker weet dat het bestaat. Je kunt het openen door een extra wachtwoord in te voeren, dat je speciaal voor de toegang tot het verborgen volume hebt gemaakt. Dit wachtwoord kun je veel langer voor je houden dan het wachtwoord van de (als willekeurig bestand) zichtbare container, omdat het volume eigenlijk niet lijkt te bestaan.

Verborgen volume binnen VeraCrypt aanmaken

1. **Creëer het volume voor de buitenschil**
   Start VeraCrypt en klik:

   - 'Create Volume' → 'Create an encrypted container' → selecteer 'Hidden VeraCrypt volume' (verborgen VeraCrypt-container) → selecteer de locatie waar de container moet worden opgeslagen (je kunt het later verplaatsen) en geef de container een onopvallende naam.

     Om een volledige externe harde schijf, zoals een USB-stick, te versleutelen, selecteer je 'Create Volume' → 'Create a volume within a partition/drive' (creëer een volume op een partitie of drive). Om de USB-drive te ontsleutelen heb je VeraCrypt ook nodig, dus als je van plan bent om bestanden te ontsleutelen op een computer waar VeraCrypt niet op is geïnstalleerd, is het verstandig om naast de versleutelde container op de USB-drive met je bestanden ook het programma VeraCrypt op de USB-stick op te slaan.

   - Het volgende venster is getiteld 'Encryption Options' (versleutelingsopties). De standaardinstellingen voldoen. Voor de sterkste encryptie (die meerdere keren versleuteld), kies je bij 'Encryption Algorithm', voor 'AES twoFish-Serpent', en bij 'Hash Algorithm', selecteer je 'SHA-512'.

   - Daarna zie je het scherm 'Volume size'. Selecteer hier de grootte van de container. De grootte bepaalt hoeveel data je in de container kunt opslaan.

   - Vervolgens word je gevraagd het wachtwoord voor het volume in te stellen. Kies een veilig wachtwoord (zie hoofdstuk 8) en … Vergeet.Deze.Niet!!!

   - Het volgende venster is getiteld 'Format Options'. Selecteer 'FAT'.

     Expert-info: FAT is compatibel met alle systemen, maar kent een maximum aan de grootte van bestanden die je kunt opslaan. Losse bestanden mogen niet groter zijn dan 4 GB). Dit zal in de meeste gevallen geen probleem zijn. Als je grotere bestanden moet kunnen opslaan en je weet zeker dat een ander format je geen problemen oplevert met het delen van de bestanden, kies dan een van de andere opties.

   - Het programma maakt nu een willekeurige dataset om het volume te versleutelen. Maak een paar willekeurige muisbewegingen (de computer kan daarmee een betere encryptiesleutel aanmaken) voordat je op 'Format' (formatteren) klikt. Vervolgens wordt het volume aangemaakt. Afhankelijk van de grootte, het gekozen encryptie-algoritme en de snelheid van je computer duurt het aanmaken een paar seconden tot een paar uur (voor zeer grote volumes).

   - Het volgende scherm is getiteld 'Outer Volume Contents' – lees dit zorgvuldig door. Je moet nu een wat bestanden die de indruk wekken gevoelige informatie te bevatten, in het buitenste volume plaatsen (het kopiëren/plakken van een aantal bestanden in de VeraCrypt-container die je in de bestandenlijst ziet. Daarna klik je op 'Next' (volgende).

   - Je krijgt nu een venster in beeld met de titel 'Hidden Volume'. Lees dit door en klik 'Next'.

2. **Creëer het verborgen volume**
   Nu het buitenste volume is aangemaakt, volg je de stappen om een verborgen volume aan te maken. Dit volgt dezelfde procedure als bij het aanmaken van het buitenste volume in de vorige stap, maar nu voor je verborgen volume. Ook hier krijg je de schermen voor 'Encryption Options', grootte van het 'Hidden Volume Size' en wachtwoord aanmaken via 'Hidden Volume Password'. Let op, de beschikbare grootte is uiteraard de grootte van het buitenste volume minus de grootte van de bestanden die je daar als afleiding in hebt geplaatst. Verder **moet*** je een ander wachtwoord kiezen voor het verborgen volume dan die van de buitenste schil. Kies vervolgens 'Format Options' (kies FAT, zie hierboven).

   * Het is belangrijk dat je een ander wachtwoord voor het verborgen volume kiest dan voor de buitenschil. Doe je dit niet, dan heb je met één wachtwoord toegang tot beide containers. De verborgen container verliest daarmee zijn functie.

3. **Plaats de bestanden die je wilt versleutelen in je verborgen volume**
   Nu kun je het volume activeren. Open je bestandenlijst. Klik op 'Select File' (selecteer bestand)> ga naar het volume dat je zojuist hebt gemaakt en selecteer deze, kies vervolgens 'Mount' (activeren). Voer het wachtwoord in voor het volume waarvoor je toegang wilt (in dit geval het verborgen volume) en klik OK.

Let op *als je later meer data in de buitenschil plaatst, kan tot gevolg hebben dat ruimte/data in het verborgen volume wordt overschreven. Let er dus op dat je geen nieuwe bestanden meer in de buitenschil plaats nadat je het verborgen volume hebt aangemaakt.*

Je kunt nu bestanden in de verborgen container plaatsen. Dat doe je op dezelfde manier zoals je dat met een USB-stick zou doen. Ga naar Mijn Computer of de Finder (Mac), selecteer de gewenste bestanden en sleep ze naar de container. Als je de bestanden in de container hebt geplaatst, kun je de container sluiten door te klikken op 'Dismount' in VeraCrypt. De container lijkt nu op een willekeurig bestand op je computer.

Encryptie van harddrives

Naast het gebruik van bestanden als VeraCrypt-containers kun je er ook voor kiezen om de complete harde schijf te versleutelen. De meeste actuele besturingssystemen hebben een ingebouwde optie om de harde schijf te versleutelen. Zorg ervoor dat je de systeembestanden en programma's op een andere schijf opslaat als je data. De schijf met de data versleutel je.

Windows
Zoek op 'Bitlocker' (Configuratiescherm\Systeem en beveiliging\BitLocker-stationsversleuteling), kies welke schijf je wilt versleutelen en stel eventueel een wachtwoord in. Je kunt er ook voor kiezen om een externe schijf of USB-stick te versleutelen met 'Bitlocker to go'.

Linux/Ubuntu
In het onderdeel Ubuntu installeren (hoofdstuk 2), geven we de instructie om de opties 'encrypt the Ubuntu installation' en 'encrypt the home folder' te selecteren. Dit zorgt ervoor dat de complete harde schijf en de home-directory worden versleuteld, beide met een ander wachtwoord.

Mac
Ga naar Systeemvoorkeuren → Security en Privacy → FileVault (kluis) → zet FileVault aan.

Data veilig delen

Risico's:

- Interceptie;
- Interventie;
- vernietiging van je brondocumenten;
- identificatie van je bron;
- identificatie van de journalist.

Infosec-actie:

- wissel versleutelde USB-drives of harddrives uit (als je elkaar in persoon kunt ontmoeten);
- wissel data van beperkte hoeveelheid uit via versleutelde bijlagen in versleutelde e-mails;
- wissel data met groter volume versleuteld uit via een filesharing-dienst (zie hierna).

Fysieke uitwisseling

De veiligste manier om grote hoeveelheden data uit te wisselen is fysiek (in persoon) een opslagmedium (bij voorkeur een USB-stick of harddrive) met daarop de data in versleutelde vorm uit te wisselen. De hele stick/drive kan worden versleuteld, of een aantal mappen kunnen worden versleuteld en beveiligd met verschillende wachtwoorden. Op die manier kan de bron op een gecontroleerde manier toegang tot de data geven, bijvoorbeeld door de wachtwoorden op verschillende momenten via veilige kanalen (zoals versleutelde mail of OTR-chat, zie hoofdstuk 5 en 6) vrij te geven. Dus, alles wat je nodig hebt voor het fysiek uitwisselen van gegevens is versleutelingssoftware (zoals VeraCrypt) en een USB-stick.

Digitale uitwisseling van data
Als jij en je bron elkaar niet fysiek, face-to-face, kunnen ontmoeten om de documenten in ontvangst te nemen, moet je je documenten op een veilige manier online uitwisselen. Kleine hoeveelheden data kunnen worden gedeeld als versleutelde bijlage bij een versleuteld e-mailbericht als je beiden e-mailencryptie gebruikt (zie hoofdstuk 5).

Grotere hoeveelheden data kunnen worden versleuteld met VeraCrypt. Je geeft het bestand een onopvallende naam die geen relatie heeft met de inhoud en vervolgens kun je het uitwisselen via een filesharing-dienst. Je kunt de ontvanger via een veilig kanaal (zoals encrypted mail of chat) een link naar het online-bestand sturen met het wachtwoord om het bestand te ontsleutelen.

Maar let op, je moet er zeker van zijn dat je een veilig systeem hebt als je de optie van digitale data-uitwisseling gebruikt. Als je hardware of je besturingssysteem niet veilig is, dan kunnen de bestanden en wachtwoorden die je deelt, gecompromitteerd zijn. Een tegenstander heeft dan wellicht op afstand toegang of zelfs controle over je computer. Bij voorkeur wissel je documenten alleen uit tussen twee veilige computers waarop je allebei Tails gebruikt. Voor de hoogste vorm van veiligheid bekijk je de documenten alleen op een airgap-computer.

Mega voor het delen van bestanden
'Mega' (https://mega.nz/) is een goed alternatief voor platforms als Dropbox en Google Drive om bestanden te delen. Mega zorgt eerst voor een bepaalde mate van versleuteling in de browser voordat het bestand wordt geüpload om zo de gebruiker te beschermen tegen nieuwsgierigen met beperkte

vaardigheid en om zichzelf te beschermen tegen beschuldigingen over het faciliteren van inbreuk op copyright (omdat ze niet weten wat de inhoud is van de bestanden die worden gedeeld). De mate van versleuteling door Mega is weliswaar niet overheidsproof, maar het geeft wel een extra laagje bescherming tegen nieuwsgierige blikken in de data als het via een open wifi-verbinding wordt verstuurd, bijvoorbeeld in het door jou gekozen café of de bibliotheek (voor het anoniem versturen van de bestanden). Zoals bij de meeste providers van online-bestandsopslag gebruikelijk is, krijg je ook bij Mega gratis opslagruimte. Mega biedt 50 GB voor elk uniek e-mailadres dat je gebruikt. Zoals met ieder ander onderdeel van informatiebeveiliging is het ook nu aan te raden om data te verspreiden over verschillende accounts die niet met elkaar in relatie staan.

SecureDrop
Sommige journalistieke organisatie met goede voorzieningen en IT-mogelijkheden, hebben hun eigen systemen gemaakt om het veilig delen van bestanden te faciliteren, waaronder SecureDrop. SecureDrop is een opensourcesysteem waar klokkenluiders documenten kunnen achterlaten en het is goed nieuws dat er organisaties zijn die SecureDrop gebruiken. Maar de juiste setup van zo'n systeem instellen en deze veilig houden is een moeilijke taak en moet niet zonder de hulp van specialisten met uitgebreide ervaring, mensen die zichzelf in het veld bewezen hebben, worden gedaan. Daarom is SecureDorp geen werkbare oplossing voor onafhankelijke journalisten.

Neem contact op met de IT-serviceprovider van je organisatie voor vragen hierover. Die kan wellicht helpen (maar vraag altijd of ze iets dergelijk eerder hebben gedaan en als dat niet zo is, vraag dan hulp aan een ander). De CIJ kan je eventueel helpen door je in contact te brengen met mensen die ervaring hebben op dit gebied.

OnionShare
https://onionshare.org

OnionShare is een opensourcetool die je veilig en anoniem via het Tork-netwerk bestanden van willekeurige grootte laat delen. OnionShare biedt een veilig systeem van bestanden delen aan, omdat het ervoor zorgt dat gebruikers bestanden rechtstreeks van computer naar computer delen, via Tor-verbindingen, zonder bestanden te uploaden naar een server van een derde. In plaats daarvan wordt de computer van de zender de server voor de uitwisseling. OnionShare is gemakkelijk te installeren en te gebruiken op zowel Windows, Mac, Ubuntu en Tails. Voor de installatie op Ubuntu moet je de command-regel beperkt gebruiken. Je kunt OnionShare hier downloaden (inclusief installatie-instructies): https://onionshare.org

Het gebruik van OnionShare: om bestanden met OnionShare te kunnen versturen, moet je je Tor-browser op de achtergrond laten draaien. Je moet de Tor-browser ook gebruiken om bestanden te downloaden via OnionShare. De zender kiest de bestanden die hij wil delen en OnionShare stelt deze bestanden beschikbaar ter download via een URL in de Tor-browser. Als de ontvanger het bestand downloadt (rechtstreeks vanaf de computer van de zender), kan de zender de voortgang en voltooiing van de download volgen.

Als je je zorgen maakt over gerichte surveillance en pogingen om je te delen bestanden te onderscheppen, wees dan voorzichtig met het delen van de URL met je contactpersoon. Je moet dat op een veilige manier doen, bijvoorbeeld via versleutelde OTR-chat of versleutelde e-mail (zie hoofdstuk 5 en 6) of anoniem, bijvoorbeeld via een nieuw anoniem e-mailaccount dat je aanmaakt via de Tor-browser en dat je na gebruik verwijdert.

Als de download is voltooid of wanneer de zender OnionShare sluit, worden de bestanden volledig van het internet verwijderd (tenzij je 'Stop sharing automatically' in OnionShare uitvinkt; hierdoor wordt het mogelijk de bestanden verschillende keren te downloaden). Meer instructies vind je hier: https://github.com/micahflee/onionshare

Bestanden veilig verwijderen

Op de meeste systemen verdwijnt een bestand niet echt van de harde schijf of USB-stick als je het verwijdert. Het bestand blijft bestaan, maar de plek waar het staat krijgt het label 'niet meer in gebruik'. Hierdoor weet het systeem dat het die plek mag overschrijven met andere data. Maar, pas tot die plek wordt overschreven, blijft het oude bestand onzichtbaar aanwezig en kan deze ook worden teruggehaald met forensische tools en ervaring.

Om ervoor te zorgen dat een bestand echt veilig en compleet wordt verwijderd, kun je een extra tool gebruiken die de ruimte waar het bestand was opgeslagen een paar keer overschrijft. Deze methode is heel veilig, maar het kan veel tijd kosten bij grotere datavolumes (dat wil zeggen, tot een aantal uren voor USB-sticks met een opslagcapaciteit van meerdere GB's).

Windows, Linux/Ubuntu
Op Linux- en Windows-systemen is BleachBit (http://bleachbit.sourceforge.net/) de belangrijkste opensource-verwijdertool die als zeer betrouwbaar staat aangeschreven.

Tails
Het Tails-systeem heeft een functie waarmee je veilig kunt verwijderen. Die kun je gemakkelijk openen als je met de rechtermuisknop op een bestand klikt en vervolgens kiest voor 'Wipe'. Je kunt alle "lege" plekken in een map veilig overschrijven/verwijderen door in een map met de rechtermuisknop te klikken en te kiezen voor 'Wipe available diskspace'.

Mac
Voor het veilig verwijderen van losse bestanden hadden de oude versies van macOS (OS X) binnen 'El Capitan' de functie 'Secure Empty Trash'. Die functie bestaat niet meer omdat men niet kon garanderen dat dit daadwerkelijke op een veilige manier gebeurde. Daarom is er op een Mac nu geen manier meer om losse bestanden op een veilige manier te verwijderen. Het is daarom belangrijk dat je de harddrive versleutelt, en toegang alleen mogelijk maakt met een wachtwoord.

Voor het veilig wissen/opschonen van een USB-stick (of willekeurige externe harde schijf): doe de USB-disk in het apparaat: start 'Disk Utility'→ selecteer de drive die je wilt wissen (kijk in het menu links) → selecteer de erase-tabe (verwijder-tab). Selecteer 'Security Options' en schuif de slider naar 'Most Secure'* → 'OK' → "Erase'.

Fysiek vernietigen van gegevens
Als een volledige disk moet worden gewist, heb je ook de optie om het opslagapparaat fysiek te vernietigen. Om er zeker van te zijn dat er geen data meer van het medium kan worden teruggehaald, moet je het apparaat in zeer kleine onderdelen, niet groter dan 1 mm, verdelen. Je kunt er dus niet van uitgaan dat je forensische technieken kunt omzeilen door bijvoorbeeld een schijf met een hamer kapot te slaan of hem in water onder te dompelen. Het apparaat werkt dan waarschijnlijk niet meer, maar het voorkomt helaas niet dat een tegenstander de data er vanaf kan halen, zeker als deze de middelen en de tijd heeft om voor het dataherstel geavanceerde technieken in te zetten.

Kies voor USB-drives
Het opslaan van data op de harde schijf van een laptop zorgt ervoor dat je data aan meer risico's blootstaan en vaak is het moeilijker om ze veilig te verwijderen. Daarom is het aan te raden om gevoelig materiaal op een extern opslagmedium op te slaan, zoals een USB-stick of een externe harde schijf (voor grotere volumes). Versleuteling van die apparaten en van de bestanden erop is ook belangrijk om ze te beschermen tegen verlies of diefstal door kwaadwillenden.

Metadata

Metadata zijn de data over data. Digitale bestanden bevatten verschillende metadata die als het ware in een schil om het bestand hangen. Je moet daarbij denken aan de auteur van een Word-document, de GPS-coördinaten van de locatie van een foto. Audio, video, en PDF-bestanden bevatten ook metadata en verborgen data (zoals commentaar, tracking-gegevens, bestandsnamen, etc.). De meeste kleurenlaserprinters printen hun type- en serienummer in onzichtbare puntjes op iedere vierkante centimeter van het papier. De herkomst van het papier of stukjes daarvan zijn dus te traceren naar de printer en uiteindelijk naar jou als die printer naar jou leidt (bijvoorbeeld als je de printer online hebt besteld). Bedenk ook dat moderne printers/copiers een harde schijf hebben waarop data wordt bewaard.

Elk programma dat je gebruikt kan specifieke metadata-instellingen hebben. Zorg er dus voor dat je weet welke informatie wordt opgeslagen in (bestanden van) het programma dat je wilt gebruiken en of en hoe je die informatie kunt verwijderen. Zo zorg je ervoor dat de metadata onschadelijk voor je zijn. Je kunt dit bijvoorbeeld achterhalen via onlineonderzoek naar het bewuste programma en de gebruikte bestandsformaten.

LibreOffice
LibreOffice is een gratis, opensource set applicatie voor het kantoor (vergelijkbaar met MS Office).
https://www.libreoffice.org/

In LibreOffice kun je gebruikersgegevens (userdata) zien en verwijderen via File → Properties → tab General (Bestand, Instellingen, tab Algemeen)

- Klik 'Reset' om algemene gebruikersgegevens te resetten (bijvoorbeeld de totale tijd gebruikt voor editen, het revisienummer, etc.)
- Vink uit 'Apply user data' (uitschakelen van het toepassen van userdata).
- Ga naar de tabs 'Description' en 'Custom Properties' om haal daar de data weg waarvan je niet wilt dat deze bekend wordt/zichtbaar is.
- Bij de tab 'Security' vink je uit 'Record changes' als dat nog niet is uitgeschakeld. Bij Edit → Changes → Accept or Reject kun je deze verwijderen als de ontvanger ze niet nodig heeft.

Als je de optie Versions gebruikt, ga je naar File → Versions. Hier delete je oudere versies van het document die wellicht zijn opgeslagen.

Voor Writer: controleer of alle verborgen paragrafen zichtbaar zijn bij Hidden Paragraphs.
Voor Calc: controleer of er geen verborgen werkbladen zijn bij Format → Sheet.

Hoofdstuk 5: e-mail

Hoogstwaarschijnlijk gebruik je e-mail het vaakst als communicatiemiddel met collega's en bronnen. Het is ook de manier waarop een nieuwe bron contact met je kan leggen. Het is daarom erg belangrijk voor onderzoeksjournalisten om veilig te kunnen e-mailen, niet alleen voor de dagelijkse dingen met collega's maar ook als veilig kanaal voor het eerste contact met bronnen.

Je loopt verschillende risico's met e-mailcommunicatie als je tegenstander je mail kan benaderen:

- je e-mailinhoud lezen;
- de onderwerpregel van je e-mail lezen;
- zien met wie je contact hebt, hoe vaak en wanneer;
- e-mailbijlagen onderscheppen;
- een zogenaamde "man-in-the-middle"-aanval (waarbij iemand zich voordoet als iemand anders en daardoor de communicatie kan onderscheppen);
- zien vanaf welke locatie je e-mailt.

Acties rondom informatiebeveiliging:

- gebruik sterke wachtwoorden;
- gebruik een betrouwbare e-mailprovider;
- versleutel je e-mail;
- verifieer je encryptiesleutels;
- zet minimale informatie in de onderwerpregel van je e-mailberichten;
- verstuur e-mail via Tails (wanneer nodig);
- gebruik van anonieme e-mailadressen voor specifieke doeleinden.

Een sterk wachtwoord is in de meeste gevallen voldoende als bescherming tegen de meeste kwaadwillenden die niet namens een overheid werken, om ongeautoriseerde toegang tot je e-mail-account te voorkomen. Maar voor een tegenstander op het niveau van overheidsdiensten biedt dat misschien geen enkele bescherming.

Een betrouwbare e-mailprovider is een provider die in de basis een goed beveiligde infrastructuur heeft in de systemen en die je data niet zomaar aan een inlichtingendienst overhandigt. Als je het land waar je e-mailprovider is gevestigd, niet vertrouwt, dan kun je beter geen e-mailadres in dat land gebruiken. We weten bijvoorbeeld dat het doel van de inlichtingendiensten van de USA en de UK is om zoveel mogelijk e-mailcommunicatie op te slaan als mogelijk. Zelfs als je denkt dat je e-mailcommunicatie niet van belang is voor deze diensten, kan dat in de toekomst wel het geval zijn en men kan dan met terugwerkende kracht inzicht in die gegevens krijgen.

Dus als je de aanpak van de USA rondom e-mail-privacy niet vertrouwt, wees je er dan van bewust dat e-mailproviders in de USA (zoals Outlook, Gmail, Riseup, etc.) de werkwijze van dat land toepassen. De ene e-mailproviders werkt daar wellicht meer aan mee dan andere, maar – tenzij je je eigen server draait of tenzij de organisatie waar je voor werkt heeft een server in een land met goede privacywetten, zoals Zwitserland of IJsland – moet je aannemen dat je e-mails en je e-mail metadata niet veilig zijn bij welke e-mailprovider dan ook. Een ander overweging bij je keuze om je account bij een provider te registreren, kan zijn of je persoonlijke gegevens wilt verstrekken, zoals je mobiele

nummer, je adres/postcode, een ander e-mailadres, omdat je wellicht in de toekomst wilt voorkomen dat die informatie bekend wordt (in het bijzonder als je een anoniem e-mailadres gebruikt).

Metadata van e-mail

Metadata zijn de data over data. Digitale bestanden bevatten verschillende metadata die als het ware in een schil om het bestand hangen. E-mail-metadata bevatten informatie over de zender en ontvanger, de e-mailadressen, gebruikte IP-adressen, serverinformatie, datum, tijd, tijdzone, unieke identificatiecode van de e-mail en gerelateerde e-mails, soort inhoud en codering, inloggegevens van de mailclient met IP-adres, informatie over prioriteiten en categorieën, onderwerp, status en leesbevestigingen.

Je ziet dat deze informatie uitgebreid en onthullend is, maar veel inlichtingendiensten en justitiële instellingen (en in sommige gevallen individuele hackers) zijn in staat de hele inhoud van de e-mail te verkrijgen.

Het is niet eenvoudig om de metadata van e-mails te beschermen, dus je moet in de onderwerpregel zo kort mogelijk zijn en/of verhullende teksten gebruiken. Het kan ook verstandig zijn om je locatie/IP-adres te verbergen door gebruik te maken van de Tor-browser.

Voorbeeld: in de zomer van 2013 vroegen autoriteiten van de Amerikaanse overheid toegang tot de metadata van een onbekende gebruiker van Lavabit, een veilige e-mailprovider. Bovendien vroegen ze de encryptiesleutels van het bedrijf (waarmee je toegang krijgt tot de wachtwoorden van de gebruiker). Waarschijnlijk vroeg men om de encryptiesleutels omdat het ze niet lukte om heimelijk toegang tot het beoogde account te krijgen. Waarschijnlijk had de poging tot onderschepping te maken met de aanname dat NSA-klokkenluider Edward Snowden een e-mailaccount bij Lavabit had. De oprichter van Lavabit werd juridisch gezien beperkt om de exacte vragen van de overheid ter discussie te stellen/te bespreken, zoals iedereen die op deze manier wordt benaderd met het verzoek om informatie (dit maakt evaluatie van de veiligheid van e-mailproviders extra moeilijk). Uiteindelijk koos de oprichter van Lavabit ervoor zijn bedrijf op te heffen in plaats van de privacy van de gebruiker in kwestie op te geven.

E-mailencryptie

Je kunt echter de privacy van je e-mailinhoud beschermen door gebruik te maken van 'public key cryptography' (publieke sleutel cryptografie). Hiermee verhaspel je de inhoud van je e-mailberichten in een (tot nu toe) onbreekbare code waarbij je de publieke sleutel van de ontvanger gebruikt. De versleutelde e-mail kan dan alleen worden ontsleuteld met de privé-encryptiesleutel van de beoogde ontvanger.

De volgende instructies gaan ervan uit dat je de aangeraden GNU Privacy Guard, 'GPG' (een opensourceversie van Pretty Good Privacy, ook wel PGP) gebruikt. Het gebruik van GPG is niet moeilijk alhoewel het erg verschilt van normaal e-mailen. Je zult er desondanks snel mee kunnen werken. Het is alleen iets lastiger te doorzien hoe het precies werkt.

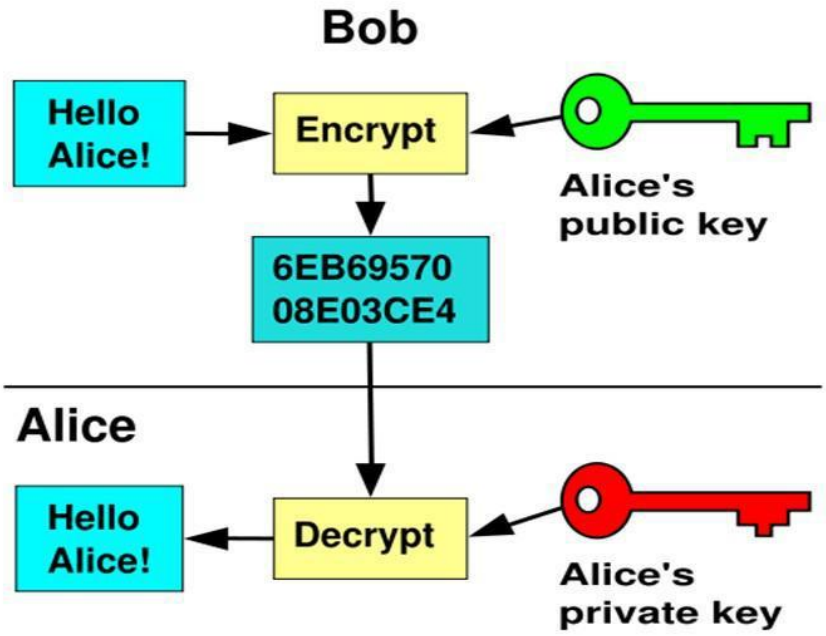
Sleutelparen (key pairs)

Sleutels zijn feitelijk unieke lange series met nummers en elke gebruiker van e-mailencryptie heeft een sleutelpaar, een publieke sleutel en een privésleutel.

Je publieke sleutel: jouw publieke sleutel wordt door mensen gebruikt om de e-mails te versleutelen die ze aan jou sturen. Je kunt het vergelijken met een lijst met telefoonnummers in een telefoonboek. Je kunt er zelf voor kiezen of je je publieke sleutel wilt tonen op de server met publieke sleutels of niet. Als je een geheim of anoniem e-mailaccount gebruikt, wil je je publieke sleutel niet op de sleutelserver publiceren. Als je ervoor kiest om je publieke sleutel te laten opnemen op de sleutelserver, wordt deze openbaar beschikbaar zodat iedereen je versleutelde berichten kan sturen.

Je privésleutel: met je privésleutel kun je e-mails ontsleutelen die anderen naar je hebben gestuurd, versleuteld met jouw publieke sleutel. Ook al is je publieke sleutel zichtbaar/beschikbaar, de privésleutel van het sleutelpaar moet altijd privé zijn. De sleutel komt overeen met je publieke sleutel waardoor je het bericht kunt ontsleutelen en waardoor je er zeker van kunt zijn dat niemand anders je publieke sleutel ongeautoriseerd kan gebruiken voor de eigen mail. Je zult je eigen privésleutel waarschijnlijk niet eens onder ogen krijgen, het leeft en werkt onder de kap van je GPG-software.

De lengte, willekeur en verfijndheid van sterke public key cryptography (sleutels van 4096 bit, zie onze instructies hierna) zijn van zo'n kwaliteit dat de encryptie, voor zover we weten, tot nu toe niet te kraken is.



Sleutels verifiëren

Het is belangrijk dat je altijd verifieert dat de publieke sleutel van de beoogde ontvanger, dus degene aan wie je een versleutelde mail stuurt, daadwerkelijk bij de ontvanger hoort. Alhoewel het e-mailadres wel klopt en toebehoort aan degene die je een bericht wilt sturen, bestaat er een kleine kans (bij een hoog risiconiveau) dat de publieke sleutel niet bij de ontvanger hoort. Dit is bekend als de 'Man-In-The-Middle'-aanval (MITM-aanval), waarbij de communicatie in het geheim wordt onderschept doordat de kwaadwillende zich als de ontvanger voordoet. Je moet je er dus van verzekeren dat zowel e-mailadres én publieke sleutel beide tot de ontvanger in kwestie behoren. Hierover lees je mee bij 'sleutelverificatie' verderop in dit hoofdstuk.

Je identiteit en locatie beschermen als je e-mailt

Degenen die hun werkelijke identiteit of die van anderen verborgen willen houden in de communicatie, bijvoorbeeld bij hoge risiconiveaus, moeten anonieme e-mailaccounts gebruiken. Dat moeten accounts zijn die niet met iets anders van die persoon online kan worden geassocieerd, op wat voor manier dan ook. Gmail en Hotmail vragen om een telefoonnummer of een alternatief e-mailadres, waardoor deze providers niet zo geschikt zijn voor anonieme accounts. Providers als GMX en Yandex staan gebruikers in veel landen toe om accounts aan te maken zonder informatie te vragen waarmee je kunt worden geïdentificeerd.

Als je een anoniem account aanmaakt, moet je rekening houden met een aantal dingen. Bijvoorbeeld als je je anonieme e-mailadres aanmaakt via een internetverbinding die met jou kan worden geassocieerd, dan is je anonimiteit niet meer gegarandeerd. Bovendien, als je e-mails stuurt en ontvangt via zo'n internetverbinding, dan is je locatie bekend bij de internetprovider (en mogelijk ook je tegenstander). Als je zowel je identiteit als je locatie anoniem wilt houden, kun je een anoniem account aanmaken en gebruiken om onversleutelde berichten te versturen via webmail in de Tor-browser (zie hoofdstuk 3). Je kunt ook het Tails-besturingssysteem gebruiken; deze verbergt de echte locatie van alle communicatie van je laptop met het internet (zie hoofdstuk 2). Tails' desktop e-mailclient (die encryptie ondersteunt) verstuurt en ontvangt informatie/mail van het internet via Tor, waardoor de echte locatie van de verbinding verborgen blijft.

Misschien wil je je locatie in het veld verbergen en niet zozeer je identiteit. Daarvoor is het gebruik van het Tails-besturingssysteem de enige oplossing.

Basisopmerkingen over encryptie van e-mail

Weet dat het versleutelen van e-mail niet de metadata verbergt, zoals met wie je mailt, de onderwerpregel, je locatie (hoewel je dat kunt verbergen als je Tor/Tails gebruikt, zoals hiervoor aangegeven), etc. Het is voor iedereen, voor alle risiconiveaus, aan te raden om voor de onderwerpregel minimaal te houden of te kiezen voor een onschuldig onderwerp dat niet gerelateerd is aan de werkelijke inhoud van het bericht.

Je kunt geen e-mail versleutelen of ontsleutelen via een smartphone. Ook al kun je zo'n systeem installeren op sommige Android-telefoons, dit is sterk af te raden omdat mobiele telefoons hoe dan ook fundamenteel onveilig zijn (zie hoofdstuk 7).

Je kunt ook geen berichten in je webbrowser versleutelen of ontsleutelen (tenzij je het Tails-besturingssysteem gebruikt). Je gebruikt de e-mailclient Thunderbird op je desktop, uitgebreid met de versleutelingssoftware voor encryptie.

Ten slotte, je kunt alleen versleutelde berichten sturen naar mensen die ook encryptie gebruiken voor hun e-mail. Dit was altijd een vrij kleine groep, maar in de post-Snowden-wereld, groeit deze groep exponentieel.

Installatie-instructies voor encryptie van e-mail (Thunderbird)

Voor encryptie van e-mail heb je de e-mailclient Thunderbird en GPG-encryptiesoftware nodig.

Ubuntu/Linux
In Ubuntu is de e-mailclient Thunderbird voorgeïnstalleerd inclusief GPG-encryptiesoftware. Gebruik de Ubuntu-zoektool van de desktop (linksboven) om het te vinden.

Mac
Je moet de volgende software downloaden:

- een e-mailclient/mailmanager voor je desktop; wij raden het opensourceprogramma Thunderbird van Mozilla aan.
  http://www.mozilla.org/en-US/thunderbird/
- GPG – de GNU Privacy Guard; dit is encryptiesoftware
  https://gpgtools.org/
  De eerste roze downloadknop 'Download GPG suite' is de meest recente versie van de software. Klik erop om het te downloaden. Voer daarna de installatiewizard uit om het programma te installeren.

Als de downloads voltooid zijn, open je Thunderbird vanuit je downloadmap en sleep je het Thunderbird-icoon naar de map Applicaties.

Windows
Je moet de volgende software downloaden:

- een e-mailclient/mailmanager voor je desktop; wij raden het opensourceprogramma Thunderbird van Mozilla aan.
  http://www.mozilla.org/en-US/thunderbird/
- GPG – de GNU Privacy Guard; dit is encryptiesoftware
  http://www.gpg4win.org/download.html
  De eerste groene downloadknop 'Download GPG suite' is de meest recente versie van de software. Klik erop om het te downloaden. Voer daarna de installatiewizard uit om het programma te installeren.

Installatie Thunderbird op Ubuntu/Linux, Mac en Windows
Klik op de download: Thunderbird Setup. Thunderbird biedt een korte installatiewizard. Selecteer de standaardinstallatie, bevestig de programmalocatie op het systeem en klik op volgende om de installatie te voltooien.

Open Thunderbird. Als je het programma voor de eerste keer opent, kun je de pop-up 'Integratie' in beeld krijgen. Sla dit over en haal het vinkje weg bij 'Doe deze controle iedere keer bij het starten van Thunderbird'.

Thunderbird zal je nu vragen je e-mailaccount te configureren en je een nieuw e-mailadres aanbieden. Sla dit over en kies voor het gebruiken van je bestaande e-mailadres. Voer e-mailadres en bijbehorende wachtwoord in die je wilt gebruiken voor encryptie. Je moet beslissen of je het wachtwoord wilt bewaren of niet. Het is veiliger als je het wachtwoord niet automatisch laat

onthouden, maar dan moet je het wachtwoord iedere keer invoeren als je het account in Thunderbird gebruikt. Klik daarna op volgende. Nu moet je te zien krijgen: 'Configuratie gevonden in Mozilla ISP database'.

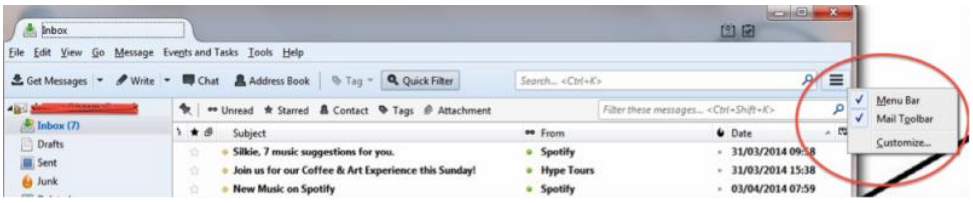
Let op – als je een anoniem e-mailadres gebruikt, voer je uiteraard niet je echte naam in.

Troubleshooting: als je het foutbericht 'Configuration cannot be verified', krijgt, gebruikt je e-mailprovider misschien een tweefactorverificatie (veel Gmail-accounts gebruiken tweestappenverificatie). In dat geval kan je provider je een e-mail sturen (of je in de webbrowser een notificatie tonen) dat er een poging is gedaan om in te loggen via een e-mailclient waarbij om authenticatie is gevraagd. Verder moeten sommige Gmail-gebruikers die tweestappenverificatie gebruiken wellicht een applicatie-specifiek wachtwoord zien te verkrijgen. Je kunt dit doen via de pagina 'autorisatie applicaties en sites' bij de instellingen van je Google-account. Voor meer informatie, bekijk: https://support.google.com/mail/answer/1173270?hl=en

Enigmail, security-extensie

Boven in het venster van Thunderbird klik je op Tools → Add-ons → Extensions. Als je hier 'Enigmail', ziet staan, is het programma al geïnstalleerd. Staat het hier niet vermeld, ga dan naar het zoekvenster rechtsboven van het venster en kies 'Enigmail'. Klik op installeren en herstart Thunderbird. Als Thunderbird opnieuw opstart, kun je de tab 'Add-ons Manager' sluiten.

Let op: als je geen menu hebt bovenin het venser van Thunderbird, klik dan met je rechtermuisknop op het icoontje met de drie regels, helemaal rechtsboven en vink aan 'Menu Bar'.



Sleutelparen
Klik bovenaan in Thunderbird op Enigmail → sleutelmanagement (Key Management). Ga naar de bovenste toolbar en klik → Genereer → nieuw key pair (sleutelpaar).

- Het e-mailadres dat je wilt gebruiken voor versleutelde mails moet geselecteer zijn.
- klik 'gebruik de gegenereerde sleutel voor de geselecteerde identiteit'. Selecteer 'sleutel vervalt over vijf jaar'.
- voer een wachtwoordzin in (dit is het wachtwoord voor je versleutelde mail en niet alleen voor je online mailaccount – het moet heel sterk zijn).
- Het 'commentaar'-venster voegt een tekst aan je publieke sleutel toe die openbaar is als je deze op de keyserver laat weergeven. Voer hier dus geen hint in voor het wachtwoord.
- Bij 'Key expiry', moet zijn aangegeven dat de sleutel over vijf jaar vervalt/expireert.
- Ga naar het tabblad 'geavanceerd' en selecteer een maximale sleutelgrootte van 4096, en kies bij sleuteltype 'RSA'.
- klik 'Genereer sleutel' en beweeg je muis over het scherm tijdens het generatieproces (dit helpt het willekeurigheidsproces tijdens de configuratie van de sleutel). Het configureren/genereren kan een paar minuten duren.

- als de sleutel is gegeneerd verschijnt er een venster waarin dit wordt aangegeven. Klik daarna op 'genereer certificaat' in dit venster. Dit creëert een certificaat waarmee je je sleutel onklaar kunt maken (kunt intrekken) in voorkomende gevallen, bijvoorbeeld wanneer je het sleutelpaar kwijt bent of als het paar is gecompromitteerd. Bewaar het intrekkingscertificaat op een veilige plaats. Vervolgens word je gevraagd om je wachtwoordzin in te vullen om dit onderdeel af te ronden.

Configureren van Thunderbird

Ga terug naar Thunderbird om een aantal instellingen aan te passen.

Instellingen voor experts

- Enigmail → Preferences (voorkeuren) → Display Expert Settings (toon expert-instellingen)
- Basic (basis) → Passphrase settings (wachtwoordinstellingen): hier moet je instellen hoe lang Thunderbird het wachtwoord voor het sleutelpaar moet onthouden.
- Sending (versturen): selecteer 'Manual encryption settings' (handmatige encryptie-instellingen) en vink aan:
    - 'Encrypt/sign replies to encrypted/signed messages' (versleutel en onderteken antwoorden aan versleutelde en ondertekende berichten)
    - 'If possible' (indien mogelijk), bij 'Automatically send encrypted' (automatisch versleutelen bij versturen)
    - 'All usable keys' (alle bruikbare sleutels), bij 'To send encrypted, accept' (accepteer om versleuteld te versturen); of vink aan 'Only trusted keys' (alleen vertrouwde sleutels) als je de mogelijkheid hebt om je sleutels van je contacten zorgvuldig te controleren en je vanaf de start van de versleutelde communicatie het vertrouwensniveau kunt instellen.
    - 'Always' (altijd), bij 'Confirm before sending' (bevestigen voor verzenden)
      Noot: dit is een goed hulpmiddel omdat het je steeds vertelt of een e-mail is ondertekend en versleuteld. Hierdoor is de kans veel kleiner dat je per ongeluk een niet-versleuteld bericht verstuurt.
- Key Selection (sleutel selecteren): vink aan
    - 'By Per-Recipient Rules' (via per-recipient regels);
    - 'By E-mail Addresses according to Key Manager', (via e-mailadressen volgens de sleutelmanager);
    - 'Manually if Keys are Missing' (handmatig als de sleutels ontbreken).
- Gevorderd: we raden aan dat je aanvinkt 'Re-wrap signed HTML text before sending' (HTML-tekst opnieuw opbouwen voor verzending), omdat HTML-teksten niet goed samenwerken met versleuteling van e-mails.
- Klik op 'Ok'.

Mappen lokaal bewaren

Het lokaal opslaan van e-mailmappen is vooral handig om concepten te bewaren. Je wilt niet dat concepten (niet-verstuurde, onversleutelde berichten) in je online e-mailmappen worden opgeslagen. Bij voorkeur sla je de teksten op je harde schijf op, zodat je meer controle hebt over de veiligheid van de inhoud.

In de menubalk aan de linkerkant van het Thunderbird-venster zie je je e-mailmappen. Onderaan zie je lokale mappen, 'Local Folders'. Klik met je rechtermuisknop en selecteer 'nieuwe map maken' (New Folder). Het aanmaken van de mappen 'verzonden' en 'concept' in de lokale mappen kan handig zijn.

Klik aan 'bewerk' (Linux) of Tools (Mac/Windows) → Account-instellingen (Settings) → kopieën en mappen (Copies & Folders). Je kunt hier aangeven waar je je berichten wilt laten opslaan. Bijvoorbeeld, bij 'concepten en templates' ('Drafts and Templates') kun je lokale mappen selecteren als de locatie waar je conceptberichten worden opgeslagen. In hetzelfde venster kun je aangeven dat je de berichten wilt versleutelen tijdens het opslaan: bewerk (Linux) of Tools (Mac/Windows) → Account-instellingen, klik op OpenPGP Security → en vink aan 'Encrypt draft messages on saving' (versleutel concept-berichten tijdens het opslaan).

E-mail in platte tekst
HTML laat zich niet goed versleutelen, dus wen eraan je berichten in platte tekst te schrijven, dus zonder opmaak. Kies bewerk (Linux) of Tools (Mac/Windows) → Account-instellingen → Composition & Addressing (opmaken en adresseren) en vink uit 'Compose messages in HTML format' (uitschakelen dat berichten in HTML worden opgemaakt).

Deel je PGP-handtekening met je contactpersonen
Je moet je versleutelde berichten altijd ondertekenen om de ontvanger te helpen met de verificatie dat jij de verzender bent. Door je PGP-handtekening te delen met degenen met wie je e-mailt – zelfs als de e-mail niet is versleuteld – help je de ontvanger die Enigmail ook gebruikt om te verifiëren dat jij de echte afzender van het bericht bent (en niet iemand die doet alsof). Als de ontvanger geen PGP-encryptie gebruikt, geeft het ondertekenen van mail aan dat je normaal gesproken PGP-encryptie gebruikt. Ontvangers die niet precies weten hoe dit werkt, begrijpen soms niet wat die handtekening betekent.

PGP-handtekening delen: kies bewerk (Linux) of Tools (Mac/Windows) → Account-instellingen → OpenPGP Security 'Enable OpenPGP support (Enigmail) for this identity' (inschakelen van OpenPGP support (Enigmail) voor deze identiteit) moet aangevinkt zijn.

Vink aan dat je standaard versleutelde berichten wilt ondertekenen ('sign encrypted messages by default'). Je kunt ook aangeven dat je niet-versleutelde berichten standaard wilt ondertekenen. Als je een bericht ondertekent, al dan niet versleuteld, dan help je de ontvanger (als deze Enigmail ook gebruikt) om te verifiëren dat jij de echte afzender van het bericht bent (en niet iemand die doet alsof). Klik op 'OK'.

Je publieke sleutel openbaar maken op de sleutelserver
Het uploaden van je publieke sleutel aar de sleutelserver is net zoiets als je telefoonnummer laten weergeven in het telefoonboek. Het zorgt ervoor dat mensen op jouw naam/e-mailadres kunnen zoeken en je publieke sleutel kunnen achterhalen, zodat ze je een versleuteld bericht kunnen sturen. Dit is in het bijzonder handig voor journalisten die willen communiceren via versleutelde berichten en die de betrouwbaarheid van hun bronnen willen beschermen. Echter, het uploaden van je publieke sleutel heeft geen toegevoegde waarde als je een account voor encryptie aanmaakt om anoniem te e-mailen die je alleen wilt gebruiken om te communiceren met specifieke personen voor wie een hoog risiconiveau geldt.

Ga naar Enigmail → Key management (sleutelbeheer). Vink aan dat alle sleutels standaard worden getoond ('Display All Keys by Default'). Klik met de rechtermuisknop op je e-mailadres en selecteer 'Upload publieke sleutel naar de sleutelserver' als je wilt dat mensen met jou in contact kunnen

komen/je versleutelde berichten kunnen sturen. De standaard sleutelserver voldoet (pool.sks-keyservers.net).

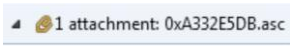
Iemands publieke sleutel zoeken
Zoek een naam of e-mailadres om te zien of iemand met een publieke sleutel staat vermeld (vergelijkbaar met het zoeken van een telefoonnummer in het telefoonboek). Je kunt ze vervolgens een versleuteld bericht versturen.

Ga naar Enigmail → sleutelmanagement → sleutelserver (in de bovenste menubalk) → zoek naar sleutels. Voer de naam van de persoon in of het e-mailadres en bekijk het zoekresultaat. Klik het e-mailadres aan van degenen van wie je de sleutels wilt importeren en klik op OK.

Een sleutel importeren
Misschien heb je de publieke sleutel van je contactpersoon al in een bestand, maar moet je deze in je sleutelmanager van Thunderbird importeren. Dat doe je als volgt.

Een sleutel via een bestand importeren: ga in Thunderbird naar Enigmail → sleutelmanagement. Ga terug naar de menubalk bovenin en klik op Bestand → importeer sleutels via een bestand.

Een sleutel importeren vanuit een e-mail: als je contactpersoon de publieke sleutel in een e-mailbijlage heeft bijgevoegd, klik dan met de rechtermuisknop op het .asc-bestand en klik in het contextmenu op 'Importeer OpenPGP-sleutel. De bijlage ziet er ongeveer zo uit:



Een sleutel importeren van een publiek sleutelblok: veel mensen vermelden hun volledige publieke sleutelblok (de volledige publieke sleutel in tekst) op hun website. Dit helpt mensen om de website te vertrouwen als de bron van de sleutel in plaats van de sleutelserver en kan ondersteunen in het voorkomen van een aanval door een tussenpersoon (man-in-the-middle, MITM).

Om de sleutel te importeren kopieer je simpelweg de volledige tekst van het sleutelblok (het volledige blok zoals hieronder is weergegeven) en plak je deze in Enigmail. Ga daarvoor in Thunderbird naar Enigmail → sleutelmanagement (terug naar de bovenste toolbar) → bewerk → importeer sleutels van het klembord → klik importeren in het bevestigingsvenster.

Voorbeeld van een compleet sleutelblok:

```
-----BEGIN PGP PUBLIC KEY BLOCK----- Version: GnuPG v1.4.11 (GNU/Linux)

mQINBFOypIgBEADEXjFLXnFDraRWa6YzzdnOSgKJKOzDSaonyQvh25lQGVOIwbg2 J1AfC+Ro3xhAxxXlkYzIwqeVIxlfNXCzZqn2KE7P0ud
F4EVrkVsWP1VcXSB65V0K 7BURi5hFFNNsk2UdnQdwcSbP77cZDkgDJofXF5hrUNlTCoLhxZ2WvpT9FfOR+Ph2 Sr/SIfcQ9K6ktsGpG5y6K
afpvtI9sI+eoSOXxDdSJyelq27mM492pcnfWjD6m1vJ 61U98CjBqLIHSrsgxVivNbRxOrler5avxZjP5+691TDRCtBIn3+2WqWrzXKfMn44
 l+iIKiqllMNJhmsuP3bEWHKGDZFk2/MafAqBWuXHOfclADX4GligLnv3EXmShlYd uKtRSPvpcCwuKgM6cVjCBrpLB+lbbq+6ILMDrTt9n4
WoV3kb5iUMV5gMrNTSdp8m Gs7zMZQFXsavlR7CjKTIFhmnPYK+v4262m7ZWvXzCVIseAtbIRYMWptzolMRSzBZ gqfcTeTQYWd1jWrbyAzi
E22wmfvUtqUlRQbh/okiCEcObHsPAr4QGtHyRBzBHkub XjHopG4E+Zh1KbHTlg/wftfKDdODDfgkrrgWkITOe6xS14OogX/Bk6Al6crn4d2
R OV36KWeVx25EfVYlmEE+62mF3GrquzxKAkx2UF7s2Jk+JIlpZUCZuMZMdwARAQAB tB5DSUogaW5mb3NlYyA8aW5mb3NlY0B0Y2lqLm9yZ
z6JAj4EEwECACgFAlOypIgC GyMFCQlmAYAGCwkIBwMCBhUIAgkKCwQWAgMBAh4BAheAAAoJEE3Wpo5++N4yJgUP /AtbshkafWk+GfNcsau
NfqSg6u4V3p8DpBTAE4oUUk753gPSJVBiGsigztmCSpxJ 6N7iqIDZ0f72AhqSlbwZ34NDPBVKrL7jRcSIwzFvTIAylMYz9eR2cWCS1ff6XM
Y+ Oac1RD+J3ksY6DfLzJfZWORAHcITuBzIgZZ47DwCGNzey0zIHS/u8w7o71C+h0WV oNFPdz1CidxCtretZkeSqvBcUNJWvx3r90Foh31o
tqhneCwrXgp1JNEZx/xKypex cReY+N6UyKQMeDOn7gj0O+fuxEqSsSx8IgtALrevm37JLz732wEZIBHiB6fh+s8i M0TpcMC//9sbL86GXG
wUdosbrGnPoCCMsgE3jDJqIVz4jEoN5XPffYCmSWNb2w9s LfQBny8s0JcRgxClytdOCDHOboBJS3ytUnUcHo/NvkpAeCEGCTvaoOtlRywdF
55p G8izK3brjKEY/1dGAx5g6aWi1iraSBOM1AHeZ/J8KOMRcEwU8sozuNeomGrSWNdR bDTaD37F0TBOzxx+QNjeSiVzleLJeHBHyZCpizX
Oe2wWEtRLq9WRHM4VUI/UGHOL xChZhwLailgkmh13eH1+47mTArbrl+P7R6Y79bmw+wld3EaE9XbnKois1on8uciW cr2qHr/PvPN8o+4hJ
7rsmsZBvX9JI+74ouyIsp0qWSrXiQIcBBMBAgAGBQJTsqfx AAoJECN9TFARig7CU2YP/igQSe8pXbJAhrQPtTk7HByHITESlrE51uFRwCVb
vTav sRN3978ob4B7QZanVlUH2YarDoLn/a90kmpECZdxlh0ZTlKKfj32jLNTWySbiQUc i/rOgli8NS7jezqauo+sB7ofPP/o3DKU4QvnRS
```

SqyIxhgae80F+mnkAOyTTWDi7H NHGq2sdLBOQALHVIVUJ5SOOEANYKZYklrR7v4iK0pc0TZDLdJ3Vm5T05N8vjCzLa TRMgNh397ElnR9n6
AGw+QRKlA21i7dAxTMecaC0nYmZx/ZVkxMRXtiSjbr2OZl63 gVxUlSo0eOjcHUX3LsX9OTew2Z+1jjaXrPJmJkxghxL/BkZx5V+knn9wTaJ
dP0r6 mO32n/lPEtG0mYeQQS4ZYbathSVqsY/QODG+7grce6mJUU3jzzo6AzfHMBRdipRb bFrnOoVsDMuu4kRvPzDXiu4kJZxZiwinDuen5
uu8//QUyuVXk1s3ATUiwUGgK8F2 CuYlut1/5E5x+MFS21IRCf2O3tFh8WIheO4BwQXErZ7FY9L7aaZa93WAcl6ueHUM IBEs06+CaPUQCcW
nxO2qwZm76aYNKwsVqptKEXcZ/mofo12/pgOjVtddLw9+4zpK Gmk2erPtMPp4eMwBkZVcRz9kGfzFn3fNanmCQ22NW5x/HFrsi/+ZSURcO/
Pcp8yk uQINBFOypIgBEADIThi9K7ioKz8vqSR3yrQ1Vp9NjPit2urzgJhW3HjLenVfvwQ1 zAoks1jDoOwuFizV9vpWpHN/ovRZqJQiKwsO
haOU8FboLrwmQMvzFaf+SrIQjVM9 YOZimEEL8a2va8M9bn8pfPO9L3beq4bWgNnxZEhEOg4ovscXUfp+ktDG/L5f5z+R 77Co07XUM8KrNc
YlDL76lKNrNumUTGJu/F+LR7LnNyRmpMi91LcyX4UkRar9xdTB /OmpwBqbH4hG3hl4xB329NL5jsCAL6gqDKIe/bD6oecWhY2GodrX9bqtw
CyMGb6/ rS+2Rv4ggwnRroRTGIlB2I+LlqRfMI2XZVZp9gt0Vj25D7LBmxyffGOFIzjtrXfG yVavBQo/cHB8uSCWlPi9bQ5ZF82f9e42Iaz
eWwrpUkyFQpiy4m8JTL2kMKt7tWEN MI2jYPIjHnhjwBGXjyAGWchM4F0TO6q+714SxtvDQKPemWqopnKbLlQSY9OzPxRv jK1iFOYLDCBu/
uYyKsll4pqr5OokRs8Q9fO9MU+jye8O48mu91vP070bHYAKvw9N 4B28acET9JlpQOHmhLWRENz4ZNap8fe1BAhHg2AE7M4ZQUS6GkPGeUcl
hZhC7vs5 /ty9IHA2bk2+fMwDr+Oye2lDife0JtbL3+krD9RLqEpSZ8SDq/BNvYJcUQARAQAB iQIlBBgBAgAPBQJTsqSIAhsMBQkJZgGAAA
oJEE3Wpo5++N4yCp8P+wW7y5fbdt/O F+4IUuVIun8yH62iQbfUBL2lrWKXaTBywyWpLvlOjfA1qy1VFZnDGoGrkc6LEhFE Wb7a53GzFyVN
SM1K/U+SF0UtdT2h0WFDqwphjtD71+L6uOve0ahRyTq0PTXnk/uT JfQ76yt7ld/6cHvvtcpYMk2n9IbeVuTWdjXLEG5Gmr4rDThUppq26oV
YG5KGCuuW s5J+k6gLPh9oNL5KKO8t8vHYbGEx3rMcdSYXXZDvYZZUDcjTE3hVXXFN3xwyHObE L20UGFJ6y3GTL2jH0iSRtquAJlMMwttey
5DOUPULu5z9prHSo961SkkZqXDhbgBp ZO6Av0Q9FyTYoxfhhf3KH5v4CivmrPZYRD/gu/doO2JGqRyWYGDYOy0E8rgNY8wJ JD9rMneDB9q
E4vsv3AmYIF5ov5dkuQe6xSTpS11h20aokru9fJvTpNNNan8A/cPu Y1Qvc06qzz0eHG4VnyAGBZ3j4cbT9BSKBtSl36aLCNa60Kzl4qLxSF
O/+wDb6dgf ToHfdTNDZT4SVjhfzoBVslNIbXzF1rgDGgBax2aR856hHfx4GERROSZZVBvPtjqy 5TrFSI9NsdNwmetMh8rxb+dz+fJYEE5y
rNs9MJPHVgeVgj0UJLawhlCGME+/lPFJ Cr8XhDwzI2n6gFvwtWQ1NNMqdn1UiF+Y =3DCe -----
END PGP PUBLIC KEY BLOCK-----

Sleutels verifiëren

Verzeker jezelf ervan dat degene met wie je denkt te communiceren daadwerkelijk degene is wie hij zegt dat hij is

Ga in Thunderbird, naar Enigmail → sleutelmanagement → klik met je rechtermuisknop op een e-mailadres → en selecteer Key Properties. Hier zie je het sleutel-ID van je contactpersoon en de PGP-fingerprint. Je kunt verifiëren dat de sleutel daadwerkelijk tot je contactpersoon behoort door de fingerprint uit te wisselen via een ander communicatiemiddel (bijvoorbeeld in persoon, via telefoon, op het visitekaartje of de website). Je moet dan checken of ze exact overeenkomen. In hetzelfde venster kun je vervolgens via Select Action → instellen in hoeverre je de eigenaar vertrouwt (Set Owner Trust) → selecteer in hoeverre je de sleutel vertrouwt die bij de betreffende contactpersoon hoort.

Een reguliere e-mailhandtekening toevoegen

Een handtekening toevoegen met je naam, functie, website, e-mailadres, PGP-fingerprint, etc.

Ga naar bewerken (Linux) of Tools (Mac/Windows) → Account-instellingen. Ga naar → Composition & Addressing en selecteer 'handtekening voor reacties toevoegen'. Hier kun je tekst bij een handtekening voor je e-mails invoeren.

Nieuwe mail ontvangen

Je kunt zelf instellen hoe vaak je wilt dat de e-mailclient de server controleert op nieuwe berichten.

Ga naar bewerken (Linux) of Tools (Mac/Windows) → Account-instellingen → Server-instellingen

Versturen van een versleuteld e-mailbericht

Als je de setup hebt voltooid, stuur je een testbericht naar iemand die ook e-mailencryptie gebruikt. Importeer zijn sleutel of zoek de sleutel op de sleutelserver en verifieer deze en geef deze contactpersoon het gewenste vertrouwensniveau toe, voordat je een e-mail probeert te versturen, anders laat de e-mailclient je misschien geen versleutelde mail sturen. Thunderbird moedigt goede informatiebeveiliging op deze manier aan.

Kies een ontvanger van wie je de sleutel al hebt geïmporteerd, geverifieerd en het vertrouwensniveau hebt ingesteld. Schrijf je bericht en voordat je het bericht verzendt, klik je eerst op het icoon met het slotje om het bericht te versleutelen en te sluiten, of ga in Enigmail naar het venster waar je het bericht

opstelt en vink ‘encryptie uit’ weg om encryptie in te schakelen. Klik vervolgens op versturen. Je moet via een bevestigingsvenster het bericht moeten krijgen dat de mail is ondertekend en versleuteld. Als dat niet zo is, ga dan terug en controleer of je ‘versleutelen’ hebt aangevinkt). Klik op ‘verstuur bericht’ en je versleutelde mail wordt verstuurd.

Nu je je contactpersoon een versleuteld bericht hebt verstuurd, kun je als standaardinstelling aangeven dat je in de toekomst alle e-mailberichten naar deze contactpersoon automatisch wilt versleutelen.

Deel je publieke sleutel met een contactpersoon
De eerste keer dat je een contactpersoon een versleutelde mail stuurt, moet je je publieke sleutel bijvoegen, zodat degene je kan beantwoorden met een versleuteld bericht. In het venster waarin je het bericht opstelt, zie je aan de rechterkant van het icoon met het slotje een icoon met een potloodje. Daar vind je de optie om de je publieke sleutel als bijlage aan je bericht toe te voegen. Selecteer deze zodat je de sleutel als bijlage mee kunt sturen bij je bericht. Een andere manier is om via Enigmail aan te geven dat je de publieke sleutel als bijlage wilt toevoegen.

Versturen en ontvangen van versleutelde bijlagen
Je kunt ook e-mailbijlagen met GPG versleutelen en ontsleutelen. Als je een bestand als bijlage stuurt bij een versleuteld bericht, kun je ervoor kiezen de bijlage ook te versleutelen. Stel het bericht op, doe het bestand er als bijlage bij en klik op versturen. Voordat het bericht wordt verstuurd, krijg je de keuze om alleen het bericht versleutelen en de bijlage(n) niet of om zowel bericht te versleutelen als bijlage(n) individueel te versleutelen. Kies de tweede optie, separaat versleutelen en ondertekenen van elke bijlage en verstuur het bericht met online PGP, klik op OK. Vervolgens komt er een bevestigings-venster, dat aangeeft dat zowel bericht als bijlagen zijn ondertekend en versleuteld. Klik op bericht versturen om het bericht met bijlage(n) te versturen.

Als iemand je een versleutelde bijlage stuurt, klik dan met je rechtermuisknop op het bestand en kies ‘ontsleutelen en opslaan als’. Sla het vervolgens op de door jouw gewenste locatie op en open het bestand vanaf die locatie.

Als je een bijlage verstuurt die al is versleuteld (bijvoorbeeld als je gebruikmaakt van VeraCrypt), dan hoef je die niet nogmaals te versleutelen met GPG.

Een nieuw account toevoegen
Het kan zijn dat je een extra e-mailaccount (met of zonder encryptie) in Thunderbird wilt gebruiken. Zo voeg je een nieuw account toe.

Ga in Thunderbird naar bewerken (Linux) of Tools (Mac/Windows) → accountinstellingen → account-acties → voeg een e-mailaccount toe.

Hoofdstuk 6: chat/instant-messaging

Instant messaging is een goede manier om communicatie met een bron te starten en te onderhouden. Het is tegenwoordig niet moeilijk om een chatapp te installeren die gebruikmaakt van versleuteling. We hebben wel wat suggesties die je privacy verhogen.

Veelgebruikte chatapps zijn WhatsApp en Facebook Messenger. Ze zijn weliswaar het meestgebruikt, maar niet het veiligst. Veiliger zijn de chatapps Wire, Signal en Telegram. De laatste twee hebben ook een desktop-versie, zodat je ze niet alleen op je telefoon maar ook op je laptop kunt gebruiken. Hier lees je welke van de drie het beste bij jou past. Overwegingen hierbij zijn bijvoorbeeld of je je telefoonnummer en/of contacten wilt delen met de app-aanbieder.

Het is ook niet moeilijk om een versleutelde 'off-the-record' (OTR) instant-messenger (IM) op je laptop te installeren en in te stellen, zeker vergeleken met de setup van mailencryptie. Als je een OTR-IM gebruikt, kun je via dat kanaal de benodigde veiligheidsprotocollen met je contactpersoon bespreken voor verdere gesprekken, ontmoetingen, e-meetings, e-mailen, het delen van documenten, etc. Het is ook een zeer bruikbare manier om met collega's te communiceren als je op afstand aan een project werkt.

OTR-IM zorgt ervoor dat je privé met iemand kunt communiceren waarbij de conversatie niet alleen is versleuteld, maar ook niet wordt opgeslagen. Daardoor kun je de conversatie ook ontkennen, in ieder geval in die zin dat het plausibel kan zijn dat een chat waarin een account staat dat met jou geassocieerd kan worden, niet van jou hoeft te zijn.

Expert-info: net zoals bij encryptie van e-mail worden bij OTR-IM ook publieke sleutels gebruikt om te verifiëren of de contactpersoon daadwerkelijk degene is wie hij zegt dat hij is. Maar iedere keer dat je een nieuwe chat begint met een geverifieerd contact, wordt de chat versleuteld met nieuwe sleutels die kunnen worden weggegooid. Geen zorgen, dat hoef je niet zelf te doen of ook maar te zien: dit zit onder de motorkap van de software (de messenger-client) die je gebruikt.

Pidgin en Adium
Als je Linux of Windows gebruikt, raden we aan dat je 'Pidgin' als IM-client gebruikt in combinatie met een OTR-plug-in. Als je een Mac gebruikt, raden we 'Adium' aan als IM-client. Gebruikers van Pidgin en Adium kunnen gemakkelijk met elkaar communiceren, maar in de huidige versie (2014) zijn de verificatiemethodes nog wel verschillend. Zie hierna bij 'contact verifiëren'.

Instructies voor het gebruik van Pidgin (voor Linux/Ubuntu en Windows)

1. **Download Pidgin en de OTR-plug-in**
   Pidgin en OTR worden in de meeste Linux-versies meegeleverd. Zoek simpelweg binnen Ubuntu (of je andere Linux-versie) naar het softwarecentrum. Zijn ze niet voorgeïnstalleerd, dan moet je ze downloaden en installeren. Werk je met Windows download en installeer Pidgin via www.pidgin.im (Windows). Werk je met Linux/Ubuntu dan word je vanaf die pagina doorgestuurd naar het Pidgin PPA-pakket. Die moet je downloaden.

   Voor Windows kun je de OTR-plug-in downloaden via https://otr.cypherpunks.ca. Voor Linux/Ubuntu ga je naar het softwarecentrum, zoek naar Pidgin OTR, en installeer de 'Pidgin Internet Messenger Off-the-record Plug-in'.

2. **Configureren van Pidgin**
   Open Pidgin. De eerste keer dat je Pidgin opent, heb je nog geen account geconfigureerd. Je krijgt daarom de vraag om een account toe te voegen. Klik op toevoegen. Krijg je de vraag om een account aan te maken niet automatisch in beeld, ga dan naar Accounts → accountbeheer → toevoegen.

   - Bedenk dat je het Pidgin-account voor anonieme communicatie het beste kunt aanmaken en verbinden met je IM-account via het Tor-netwerk. Daarmee bescherm je je ware locatie en dat is belangrijk als je het account anoniem wilt gebruiken. Bij het tabblad Proxy, selecteer 'verbinding maken via proxy' en kies 'SOCKS5' uit het dropdownmenu. In het veld 'server' typ je '127.0.0.1' en in het veld 'Poort' type je '9150'. Gebruikersnaam en het wachtwoord zijn optioneel, maar als je ze gebruikt, gebruikt Tor verschillende kanalen voor dit account in Pidgin dan voor andere onderdelen. Hierdoor wordt je anonimiteit vergroot. Let op dat je je Tor-browser open moet hebben als je verbinding wilt maken met je account (zie hoofdstuk 3).

   - in het tabblad 'Basis' selecteer je XMPP/Jabber (NIET Facebook XMPP) bij 'Protocol'. Bij Jabber kies je een (anonieme) gebruikersnaam. Bij domain typ je het geselecteerde domein (bijvoorbeeld jabber.ccc.de) – kijk hier voor een volledige lijst met mogelijke domeinen: https://list.jabber.at. In het veld 'Resource', typ je 'anonymous'. Maak een sterk wachtwoord aan (zie hoofdstuk 8).

   - Klik op het tabblad 'Geavanceerd' en controleer of 'Require encryption' (versleuteling vereisen) is aangevinkt bij 'Connection security' (veiligheid van de verbinding).

   - Ga terug naar het tabblad 'Basis' en controleer of 'Create this new account on the server' (maak dit nieuwe account aan op de server) onderaan het venster is aangevinkt, voordat je het account toevoegt ('Add').

3. **Maak een IM-account**
   Je Jabber-adres moet verschijnen in een venster 'Accounts'. Vink het 'Enabled'-vakje aan en klik op 'registreren' in het venster 'Register New XMPP Account' dat verschijnt.

4. **Configureren van OTR**
   In Pidgin, ga naar Tools → Plugins → vink aan 'Off-the-record messaging'. Klik daarna op 'Configure plug-in' om de plug-in te configureren. Vink alle standaard-OTR-instelling aan: Enable private messaging; Automatically initiate private messaging; Require private messaging, en Don't log OTR conversations. Klik vervolgens op 'generate' om een sleutel voor je account te genereren. Ga ten slotte naar Tools → Preferences (voorkeuren) → Logging, en vink alle opties uit om de chats te loggen, want je wilt niet dat er informatie van de chats wordt opgeslagen.

Gefeliciteerd! Je kunt nu off-the-record, versleuteld chatten.

Instructies voor het gebruik van Adium (voor Mac)

1. **Download Adium**
   Download en installeer 'Adium' voor Mac via http://adium.im/

2. **Creëren en configureren van een IM-account**
   Als je Adium hebt gedownload, open je het programma en ga je naar (bovenaan) 'File' → 'Add account' (account toevoegen) → 'XMPP'.

   - Bedenk dat je voor anonieme communicatie het Adium-account het beste via het Tor-netwerk kunt aanmaken en verbinden met je IM-account. Daarmee bescherm je je ware locatie en dat is belangrijk als je het account anoniem wilt gebruiken. Bij het tabblad Proxy, selecteer 'verbinding maken via proxy' en kies 'SOCKS5' uit het dropdownmenu. In het veld 'server' typ je '127.0.0.1' en in het veld 'Poort' type je '9150'. De gebruikersnaam en het wachtwoord zijn optioneel, maar als je ze gebruikt, zal Tor andere kanalen voor dit account in Pidgin gebruiken dan voor overige onderdelen, waardoor je anonimiteit wordt verhoogd. Let op dat je je Tor-browser open moet hebben als je verbinding wilt maken met je account (zie hoofdstuk 3).

   - Bij het tabblad 'Account' kies je een (anonieme) naam en je voegt op het laatst een domein voor je Jabber-ID (bijvoorbeeld @jabber.ccc.de is populair – voor een volledige lijst met mogelijkheden kijk je hier https://list.jabber.at). Een volledig Jabber-ID ziet er bijvoorbeeld zo uit:, kissinger@jabber.ccc.de. Kies een sterk wachtwoord bij 'password' (zie hoofdstuk 8). Registreer je account nog niet.

   - In het tabblad 'the Options' vink je zowel 'Require SSL/TLS' als 'Do strict certificate checks' aan. Bij 'Resource', typ je 'anonymous'.

   - In het tabblad 'Privacy' en bij 'encryption' in het dropdownmenu klik op 'Force encryption and refuse plain text' (de laatste in te lijst) om versleuteling af te dwingen.

   - Ga terug naar het tabblad Account en klik 'register account'. Er verschijnt een nieuw venster met 'server'. Typ hier het domein dat je eerder hebt geselecteerd (bijvoorbeeld 'jabber.ccc.de', of dat wat je hebt gekozen) en klik op 'Request new account' (vraag een nieuw account aan). Het account wordt vervolgens aangemaakt. Dat gaat meestal vrij snel.

3. **Adium configureren**
   Ga naar Adium → Preferences (voorkeuren) → General (algemeen) → en vink uit 'Log messages' om te voorkomen dat er gegevens van de chats worden opgeslagen.

Gefeliciteerd! Je kunt nu off-the-record, versleuteld chatten.

Beginnen met OTR-chat

Voeg een contact toe

Pidgin: in Pidgin, ga naar Buddies → voeg een buddy toe en typ zijn volledige adres in voordat je op toevoegen klikt. Als je contactpersoon de volgende keer online is, krijgt deze een autorisatieverzoek van je. Om een gesprek te beginnen dubbelklik je op de buddy/contactpersoon in de lijst. Daarna klik je OTR → 'start privégesprek' in het chatvenster.

Adium: in Adium, ga naar Contact in de bovenste toolbar → voeg contact toe. Bij 'Contact type' – aangenomen dat je contactpersoon ook Jabber gebruikt – selecteer je XMPP/Jabber, je voegt het volledige adres in bij 'Jabber ID', en je klikt op toevoegen.

Authentificatie/verificatie van een contactpersoon
Bij voorkeur gebruik je fingerprint-verificatie en als je de contactpersoon goed genoeg kent, kun je elkaar ook een vraag stellen waarop alleen de andere persoon het antwoord weet.

Authentificatie in Pidgin

Als je je contactpersoon nog niet hebt geauthentificeerd, dubbelklik op zijn adres om een chatvenster met het te openen. Ga naar OTR in het chatvenster en klik op 'Buddy authentificeren'. Je kunt op de volgende manieren authentificeren:

- vraag en antwoord, een goede, gepersonaliseerde methode
- een gedeeld geheim (dit moet van tevoren zijn geregeld via een ander communicatiemiddel, dus dit is minder goed bruikbaar)
- handmatige fingerprint-verificatie, een bruikbare, sterke methode en de enige methode waarmee Adium- en Pidgin-gebruikers elkaar kunnen authentificeren

Selecteer 'Handmatige fingerprint-verificatie' als de methode die je wilt gebruiken en je zie de fingerprint van je contactpersoon. Controleer of de fingerprint in orde is, selecteer vervolgens 'Ik heb geverifieerd dat dit inderdaad de juiste fingerprint is' en klik op authentificeren.

Authentificatie in Adium

Als je je contactpersoon nog niet hebt geauthentificeerd, dubbelklik op zijn adres om een chatvenster met hem te openen (ook als de contactpersoon offline lijkt; de zichtbaarheid van de contactpersoon blijft offline en 'niet-geautoriseerd' totdat je hem hebt geverifieerd). Klik op het icoontje met het slotje en selecteer 'Initiate Encrypted OTR chat'. Het slotje moet nu dichtgaan. Met het chatvenster open, ga je naar de bovenste toolbar in Adium, klik op Contact → Encrypti→ Verifieer. Nu krijg je de fingerprint van de contactpersoon te zien.

Het checken van fingerprints
Je moet elkaars fingerprints bij voorkeur via een ander communicatiemiddel verifiëren dan via IM. Bijvoorbeeld via e-mail of telefoon. Als je geen veilige methode hebt om dat te doen, kan een gezamenlijke vriend of derde partij een deels gewijzigde versie van je fingerprint doorsturen naar je contactpersoon (e.g. 0---A7-0 D—706-D 2—65--1 --3D-9C2 0-57B—1), en omgekeerd naar jou. Nu kun je beide de getoonde fingerprint vergelijken met de print die de tussenpersoon stuurde. Door een deel van de fingerprint te wijzigen kan een man-in-the-middle-attack worden voorkomen.

Je eigen fingerprint opzoeken
Adium-gebruikers kunnen hun fingerprint vinden via → voorkeuren → geavanceerd (de horizontale tab) → Encryptie (tab in de linkerkolom). Pidgin-gebruikers kunnen hun fingerprint vinden door een chatvenster te openen met een contactpersoon, vervolgens te klikken op het kleine buddy-icoontje (rechts van OTR) → Re/Authenticate buddy → handmatige fingerprint-verificatie'.

Let op: sta Adium en/of Pidgin niet toe om je Jabber-wachtwoord automatisch te laten onthouden, omdat deze dan misschien niet veilig wordt opgeslagen. Je moet je Jabber-wachtwoord steeds handmatig invullen elke keer als je inlogt.

Hoofdstuk 7: bellen (telefoon, voice, video) via internet

Mobiele veiligheid

Velen van ons vinden smartphones belangrijk in het dagelijkse leven, zowel privé als op het werk. Het heeft veel voordelen om steeds online te zijn en toegang te hebben tot e-mail, webbrowsers, sociale media, en agenda's. Ook de hoge kwaliteit van de meeste camera's en de voicerecorder maken smartphones waardevolle hulpmiddelen. Maar, het zijn geen gemakkelijk te beveiligen hulpmiddelen.

Als alternatief kun je met enige zorg een prepaid wegwerptelefoon kiezen, maar ook daaraan kleven risico's (zie hierna).

Risico's mobiele telefoons

- automatisch loggen van je huidige en vorige locaties;
- automatisch verzamelen van metadata (telefoonnummer, locatie van iedere beller, unieke serienummers van de betreffende telefoons, tijd/lengte van een gesprek, kaartnummers van prepaidkaarten, etc.;
- diefstal en verlies van data;
- op afstand toegang krijgen tot data als de telefoon verbonden wordt met publieke wifinetwerken;
- op afstand toegang krijgen tot alle datum op enig moment dat de telefoon aan staat;
- het aftappen van telefoongesprekken en voicemail, onderscheppen of opnemen;
- geheime automatische toegang op afstand tot de microfoon om geluid op te nemen;
- geheime automatische toegang op afstand tot de camera om foto's te maken.

Dragnet-telefoonsurveillance (sleepnet)
Alle telefoons lekken een enorme hoeveelheid informatie over ons naar inlichtingdiensten. Via de onthullingen via Snowden weten we dat er programma's worden ingezet die de volledige audio van ieder telefoongesprek binnen een land vastleggen, of in ieder geval dat dit worden getest in een aantal landen. Dit type surveillance is extreem gevaarlijk voor democratie, en dus voor journalistiek. Het maakt het mogelijk om met terugwerkende kracht het meest indringende onderzoek naar personen te doen die interessant worden voor inlichtingendiensten op een bepaald moment in de toekomst.

Het is dus de moeite waard je telefoongebruik af te stemmen op jouw situatie. Overweeg bijvoorbeeld of het gebruik de moeite waard is als jij, je bronnen of collega's doelwit van intelligentiediensten kunnen worden nu of in de toekomst. Mobiele telefoons zijn geen veilige communicatiemiddelen, dus bedenk goed hoe je ze wilt gebruiken.

Gerichte telefoonsurveillance

Laag risico
Bij lage risiconiveaus is de dreiging vooral fysiek: iemand krijgt je telefoon in handen. Als dit gebeurt, kan zelfs een minder vaardige hacker of de politie je wachtwoord kraken (als je een wachtwoordslot hebt ingesteld). Dit biedt dus minimale protectie. Als je opereert op een laag risiconiveau, zorg er dan voor dat je je data back-upt en video of audio die wordt opgenomen zo snel mogelijk opslaat naar een veilig opslagmedium (in de cloud).

Je kunt ook tracking-apps gebruiken om je telefoon terug te vinden als deze wordt gestolen. Apple biedt bijvoorbeeld voor iPhones een gratis app aan, genoemd 'Find my iPhone'. Die vertelt je op welke locatie de telefoon zich op dat moment bevindt. Een andere anti-diefstal-app is 'Prey'. Deze rapporteert de telefoon als gestolen en slaat niet alleen de huidige locatie op, maar ook de locaties waar de telefoon is geweest nadat de telefoon als gestolen is gemeld.

Gemiddeld risiconiveau
Gaat het om een gemiddeld risiconiveau, dan kun je te maken krijgen met een tegenstander die niet alleen fysiek, maar ook op afstand toegang tot je data probeert te krijgen. Als je je telefoon bijvoorbeeld met een openbaar wifinetwerk verbindt, dan kan ook een minder vaardige hacker veel informatie over jou en je accounts (zoals e-mail en sociale media) onderscheppen. Daarom moet je er bij een middelmatig risiconiveau over nadenken of je smartphones liever niet gewoon vermijdt als middel voor je werk. In ieder geval moet je de telefoon goed bewaken, bij je in de buurt houden, applicaties afsluiten/uitloggen na gebruik en de wifi van de telefoon in openbare gelegenheden uitschakelen en vliegmodus gebruiken als je niet verbonden hoeft te zijn.

De kwetsbaarheden van smartphones zijn heel uitgebreid, sommige zitten in de hardware en die kunnen niet worden aangepast/weggehaald. Je kunt opensource op je smartphone gebruiken en applicaties voor versleutelde chat (zoals Wire of Signal). Echter, zoals je kunt lezen in het onderdeel 'systeembescherming' in hoofdstuk 1: als hardware kwetsbaar is, kan de software nooit echte veiligheid bieden. Daarom gaan we verder niet in op dergelijk apps voor de smartphone in dit handboek.

Uit een telefoonhacking-schandaal in het Verenigd Koninkrijk in 2014 is gebleken dat minder vaardige hackers, die voor onethische journalisten werkten, vrij eenvoudig de voicemail van mensen wisten af te luisteren. Privédetectives hebben vaak de mogelijkheid om telefoons te tappen (dus in het geheim meeluisteren). Daarbij gaat het niet alleen om voicemail, maar ook om algemene telefoontjes die door een nummer worden ontvangen en gemaakt. Je moet er daarom goed over nadenken voordat je gevoelige onderwerpen via je mobiele telefoon of je vaste telefoonlijn bespreekt.

Hoog/top risiconiveau
Werk je op een hoog risiconiveau, dan is je telefoon in feite je tegenstander. De telefoon slaat in ieder geval je locatie op en alle met het apparaat geassocieerde metadata is in de handen van de Vijf-Ogen-inlichtingendienst (Five Eyes: een wereldwijde surveillance-afspraak waaraan vijf landen - USA, UK, Canada, Australië en Nieuw Zeeland – meedoen, ook wel bekend als de FVEY). In het ergste geval wordt de telefoon gebruikt om in het geheim alle content van je telefoongesprekken te verzamelen (nog los van alle andere data op je telefoon), en om in het geheim je microfoon en camera in te schakelen om foto's te maken en audio op te nemen. Dit soort telefoonsurveillance is vrij eenvoudig te realiseren en kost vrijwel niets voor de FVEY.

Wegwerptelefoon

Als alternatief kun je met enige zorg een prepaid wegwerptelefoon kiezen en voor je communicatie gebruiken. Een wegwerptelefoon is goedkope, contant betaalde telefoon met weinig techniek en met een prepaid simkaart die niet op je naam staat. De telefoon gebruik je alleen voor specifieke doeleinden. In sommige landen is het moeilijk om een simkaart te kopen zonder registratie van je persoonlijke gegevens. Daarom is het beter om deze tweedehands te kopen of een ander de simkaart te laten aanschaffen voor jou.

Als je een doelwit bent, zorg er dan voor dat je wegwerptelefoon en je gewone telefoon nooit allebei tegelijkertijd signalen uitzenden, want je gewone telefoon pikt het signaal van de wegwerptelefoon op. Die telefoon wordt daardoor ook een doelwit. Voordat je een wegwerptelefoon gaat gebruiken, zorg je ervoor dat de telefoon die normaal gesproken met jou wordt geassocieerd (dus je smartphone) geen signalen uitzendt. Het is normaal gesproken goed om dat te doen door de telefoon in vliegmodus te zetten, de batterij te verwijderen (als dat kan) of de telefoon uit te zetten, maar het is niet genoeg als je doelwit bent. Doe dan al deze dingen én doe het apparaat dan in een Faraday-kooi of –tas (metalen omhulsel dat signalen tegenhoudt). Populaire oplossingen daarvoor zijn beschuitbussen, bepaalde koelkasten of een roestvrijstalen cocktailshaker. De telefoon moet compleet in het metaal zijn ingesloten. Je kunt checken of de signalen worden geblokkeerd door te proberen de telefoon te bellen als deze nog aan staat en in de Faraday-kooi zit. Het is aan te raden om als Faraday-kooi een klein metalen busje met je mee te nemen om je telefoon in te doen. Zorg ervoor dat iedereen die bij een belangrijke bespreking is, hetzelfde doet (een groter metalen opbergblik werkt dan goed).

Nadat je de telefoon enige tijd hebt gebruikt, kan de telefoon met jou geassocieerd worden en doelwit worden van surveillance. Op dat moment moet je de telefoon vernietigen en een nieuwe gebruiken. Let op, het is niet genoeg om alleen de simkaart te veranderen. Iedere mobiele telefoon heeft een IMEI (International Mobile Equipment Identity), en met dat nummer wordt de telefoon geïdentificeerd. Als de SIM met jou wordt geassocieerd, doet de IMEI dat ook. Je moet dus de hele telefoon vernietigen. Vanwege de mogelijkheden van inlichtingendiensten om volledige audio-opnames te maken van alle telefoongesprekken, nog los van het gemak waarmee ze de telefoongesprekken van een doelwit kunnen opnemen, moet je voorkomen specifiek gevoelige informatie te delen in een gesprek, dus je deelt ook geen gevoelige informatie als je communiceert met een wegwerptelefoon.

Waarschuwing: inlichtingendiensten ontwikkelingen steeds meer methodes om wegwerptelefoons toch te identificeren, bijvoorbeeld door het scannen/controleren van datapatronen in bulkcommunicatie op afwijkingen. Het vermoeden bestaat dat openbare telefooncellen op dezelfde manieren worden gesurveilleerd. Je moet daarom het risico goed inschatten voordat je een wegwerptelefoon gebruikt om met een bron van een hoog risiconiveau te communiceren.

Voice- en videobellen via internet

Software waar je mee kunt voice- en videobellen via het internet zoals VoIP (Voice over Internet Protocol) en Skype, zijn enorm populair en handig. Skype heeft miljoenen gebruikers. Maar, Skype biedt weinig veiligheid en er is nog geen ander gebruikersvriendelijk, veilig alternatief. Uit de onthullingen van Snowden blijkt dat de NSA de mogelijkheid heeft om Skype-communicatie te onderscheppen en op te slaan. We moeten daarom aannemen dat alle Skype-communicatie niet alleen tussen jezelf en je contact blijft, maar dat deze ook bij de inlichtingendiensten terechtkomt.

Voorbeeld: Glenn Greenwald vertelde dat hij Skype in Hong Kong gebruikte om zijn partner David Miranda in Rio te vertellen dat Miranda versleutelde berichten via e-mail zou ontvangen van Greenwald met het verzoek deze veilig op te slaan. Greenwald heeft die bestanden nooit gestuurd, maar binnen 48 uur was de laptop van Miranda uit het huis in Rio gestolen.

We moeten ook aannemen dat niet alleen de meest ontwikkelde diensten geheime toegang hebben, of gebruikmaken van kwetsbaarheden in systemen. Van bijvoorbeeld de geheime politie van Egypte is bekend dat zij tools heeft aangeschaft om Skype mee binnen te dringen en er zijn aanvallen via man-in-the-middle op Skype gerapporteerd door milieuactivisten in Azië.

Hoofdstuk 8: wachtwoorden

Alle systemen, programma's en tools die in dit boek zijn beschreven, maken gebruik van wachtwoorden om geautoriseerde gebruikers te identificeren en te beveiligen tegen ongeautoriseerde toegang. Sterke wachtwoorden zijn de sleutel in beveiliging op alle niveaus van informatiebeveiliging.

Je moet daarbij wel in gedachten houden dat wachtwoorden tot online-accounts vooral een beveiligingsmiddel zijn tegen hackers die niet in opdracht van de overheid werken. Ook deze hebben overigens steeds vaker de beschikking over uitgekiende commerciële programma's die wachtwoorden kunnen kraken. Op overheidsniveau kan men wellicht toegang tot je online-accounts krijgen via een achterdeur, waardoor een wachtwoord onbelangrijk wordt. Daarom is het goed om je e-mailberichten te versleutelen. Je kunt nog zo'n sterk Hotmail-wachtwoord hebben, maar dat houdt inlichtingendiensten niet tegen om Hotmail te dwingen je e-mails te overhandigen (of waarschijnlijker dat ze in het geheim je berichten onderscheppen en ze verzamelen zonder toestemming). Als je e-mails versleuteld zijn, kan Hotmail alleen een berg code overhandigen die (tot nu toe) niet te kraken is.

Dus, ook al is het gebruik van sterke wachtwoorden online-accounts verstandig, de wachtwoorden die je systeem (versleuteling harddisk) en je versleutelingsprogramma's beschermen zijn veel belangrijker.

Risico's:

- vergeten of kwijtraken van wachtwoorden;
- wachtwoorden omzeilen door het gebruik van achterdeurtjes (online-accounts);
- gehackt worden (relatief eenvoudig hacken van wachtwoorden);
- kraken van wachtwoorden (verfijnd);
- keylogger die toetsaanslagen vastlegt;
- gedwongen worden om een wachtwoord vrij te geven.

Infobeveiliging-acties:

- leer hoe je sterke wachtwoorden kunt maken;
- gebruik de KeePassX-wachtwoordmanager (als je je systeem vertrouwt). KeePassX is een opensource-wachtwoordmanager die gebruikersnamen en wachtwoorden kan genereren en opslaan in een versleutelde, lokale database. De toegang wordt beschermd door een hoofdwachtwoord. KeePassX-manager is beschikbaar voor Windows, Mac, Linux en Tails;
- bewaar de belangrijkste wachtwoorden alleen in je geheugen;
- gebruik verborgen volumes voor belangrijke versleutelde bestanden.

Kraken van wachtwoorden: het risico begrijpen

Als je systeem onveilig is, is het niet moeilijk om er een gerichte aanval op uit te voeren om wachtwoorden te kraken. Een kwaadwillende kan fysiek of op afstand een keylogger in je systeem aanbrengen, om zo alle toetsaanslagen vast te leggen. Dat betekent dat een tegenstander alles kan zien wat je typt, waaronder je wachtwoorden. Zo'n aanval is niet erg moeilijk, maar het haalt alle andere beveiligingsmaatregelen onderuit. Daarom is het belangrijk om je systeem van tevoren te beveiligen, zoals eerder beschreven in hoofdstuk 1 en 2.

Een kwaadwillende kan geen keyloggers gebruiken mits je systeem goed is beveiligd. In dat geval zal de aanvaller proberen de wachtwoorden van je systeem, software en accountants te kraken. Dat kan via een grote aanval op duizenden gebruikers of via een gerichte aanval op een individu. Programma's waarmee wachtwoorden kunnen worden gekraakt, worden wereldwijd door autoriteiten gebruikt, maar er zijn ook uitstekende commerciële kraakprogramma's verkrijgbaar. Zo'n programma kan automatisch ten minste acht miljoen wachtwoorden per seconde proberen en kan dagen achterelkaar draaien, zelfs op verschillende machines tegelijk. Voor een doelwit met een hoog risiconiveau zou men het programma bijvoorbeeld maandenlang op verschillende machines kunnen draaien.

Werking wachtwoordkraakprogramma
Wachtwoordkraakprogamma's proberen eerst de meest gebruikelijke wachtwoorden. Een gemiddeld wachtwoord bestaat uit een basis en een toevoeging. De basis is niet per se een woord uit het woordenboek, maar het is meestal een woord dat je kunt uitspreken. Een toevoeging is meestal een achtervoegsel/suffix (in 90% van de gevallen), soms een voorvoegsel/prefix (in 10% van de gevallen). Een kraakprogramma begint met een woordenboek waarin ongeveer 1.000 veelgebruikte wachtwoorden staan, zoals "welkom", "letmein," "temp," "123456," etc. om deze vervolgens te testen met ongeveer 100 gebruikelijke achtervoegsels zoals "1," "4u," "69," "abc," "!," etc. Men schat dat ongeveer een kwart van alle wachtwoorden kunnen worden gekraakt met slechts 100,000 combinaties.

De kraakprogramma's maken gebruik van verschillende woordenboeken: Engelse woorden, namen, buitenlandse woorden, fonetische patronen etc. voor de basiswoorden en twee cijfers, datums, losse symbolen etc. voor achtervoegsel. De woordenboeken draaien met raadstrategieën waarbij verschillende posities van hoofdletter en algemene vervangingen zoals "$" for "s", "@" for "a," "1" for "l", etc. worden gebruikt. Deze raadstrategieën kraken al snel zo'n twee derde van alle wachtwoorden.

Een goed programma test ook namen en adressen uit het telefoonboek (postcodes worden vaak gebruikt als toevoeging), belangrijke datums en willekeurige andere persoonlijke informatie. De aanvaller kan bovendien de persoonlijke informatie van het doelwit die hij tot zijn beschikking heeft, in het programma invoeren als extra hulpmiddel.

Een bijzonder slimme aanval kan worden uitgevoerd als je hardware onvoldoende is beveiligd (dit is de basis van alle problemen!). Een aanvaller kan de harde schijf van het doelwit indexeren en zo een woordenboek maken waarin alle strings inclusief verwijderde bestanden worden opgenomen. Als je je wachtwoord ooit in een bestandje ergens hebt opgeslagen of je programma heeft het op enig moment in het geheugen opgeslagen, dan wordt het in dit proces opgepikt om te helpen het wachtwoordkraakproces te voltooien.

Zo maak je een sterk wachtwoord

Een sterk wachtwoord is een wachtwoord dat niet wordt opgepikt via het hiervoor beschreven proces van wachtwoorden kraken.

Wachtwoordmanager
Een optie om sterke wachtwoorden te genereren is het gebruik van software voor wachtwoord-management zoals KeePassX. Zo'n programma kan een willekeurig, lang, alfanumeriek wachtwoord maken (met symbolen, als deze zijn toegestaan voor het specifieke wachtwoord). De wachtwoorden worden bewaard in je eigen versleutelde wachtwoorddatabase. Als je je systeem vertrouwt, dan is het gebruik van deze software een redelijk robuuste optie.

Met een wachtwoordprogramma kun je bovendien verschillende moeilijke wachtwoorden voor verschillende accounts opslaan. Bijvoorbeeld KeePassX heeft een invoerveld voor het onthouden van de bijbehorende URL's, het invoeren van commentaar en het onthouden van de accountnamen. Je kunt dus alle informatie die je nodig hebt veilig opslaan. De gegenereerde, willekeurige wachtwoorden die het programma aanmaakt zijn te moeilijk om uit het hoofd te leren, en dat is een al een veiligheidsfunctie op zichzelf. Maar je kunt de wachtwoorden wel gemakkelijk kopiëren en plakken vanuit de database, waardoor je ze niet hoeft over te typen.

Er is wel enige discussie over hoe effectief programma's als KeePassX een willekeurig wachtwoord kunnen maken, maar daar staat tegenover dat de mens er in ieder geval niet erg goed in is. Hierdoor blijft een wachtwoordgenerator een van de beste opties die er op het moment zijn om een sterk wachtwoord aan te maken.

Voor KeePassX moet je een sterk hoofdwachtwoord aanmaken dat je wél kunt onthouden en verder nergens bewaart. In een artikel van The Verge van december 2017 wordt uitgelegd dat het ook belangrijk is om adblockers te activeren, omdat die tegenwoordig soms ook scriptjes gebruiken waarmee gebruikersnamen en wachtwoord via formulieren in browsers worden opgepikt als je de autofill gebruikt.

Het gebruik van KeePassX (wachtwoordmanager)

Toelichting: KeePassX is een wachtwoordmanager dat gebruikersnamen en wachtwoorden in een lokale database bewaart met encryptie, beschermd door een hoofdwachtwoord. Tails bevat ook PWGen, een sterke wachtwoordgenerator. Je vindt KeePassX in Applications → Accessories → KeePassX.

Een nieuwe database voor wachtwoorden maken
File → New database.
Maak een sterk hoofdwachtwoord aan waarmee je de wachtwoordendatabase kunt openen. Vervolgens geef je het databasebestand een naam en je kiest de locatie waar de database moet worden opgeslagen: Groups → New groups ('Jabber' group, voor je Jabber-gebruikersnamen en –wachtwoorden, meer over Jabber vind je in hoofdstuk 6).

Een wachtwoord toevoegen - Klik op een groep → Entries → Add new entry. Hier kun je zelf een wachtwoord invoeren of een willekeurig wachtwoord genereren (klik 'Gen' voor genereren). Als je op het icoontje met het oogje klikt kun, je de tekst van het wachtwoord zien. Doe je dat niet dan blijft het verborgen; de karakters worden als puntjes weergegeven.

Een wachtwoord opzoeken - Als je een wachtwoord aan een groep hebt toegevoegd, kun je met je rechtermuisknop klikken op het wachtwoord dat je nodig hebt. Vervolgens selecteer je 'copy password to clipboard'. Vervolgens kun je het plakken in een inlogformulier.

Schneier-schema om wachtwoorden te onthouden

Om je systeem, versleutelde USB-stick of zeer belangrijk bestand (zoals brondocumenten) te beveiligen, moet je handmatig aangemaakte wachtwoorden gebruiken die je nergens bewaart of opschrijft, maar alleen onthoudt. Daarnaast moet je voorkomen dat je een wachtwoord voor verschillende onderdelen hergebruikt, omdat je daarmee voorkomt dat een kwaadwillende toegang tot meer onderdelen krijgt als dat ene wachtwoord bekend wordt.

Zo'n wachtwoord moet dus ingewikkeld zijn, maar ook te onthouden. Om dit te bereiken, raden we de methode van het 'Schneier-schema' aan. Dit is een methode die is ontwikkeld en wordt aangeraden door Bruce Schneier, een gerenommeerde, internationaal bekende cryptograaf en security-expert.

Schneier adviseert om een zin te kiezen die je kunt onthouden, die je kunt initialiseren, symboliseren en waarin je de woorden kunt nummeren om er zo een sterk wachtwoord van te maken. Bijvoorbeeld, "This little piggy went to market" kan worden "tlpWENT2m". Zo'n wachtwoord met negen karakters staat in geen enkel woordenboek. Kies je eigen zin, iets persoonlijks maar niet iets dat duidelijk aan je publieke gegevens is gerelateerd.

Hier zijn een aantal voorbeelden:

WIw7,mstmsritt... = When I was seven, my sister threw my stuffed rabbit in the toilet
Wow...doestcst = Wow, does that couch smell terrible
Ltime@go-inag~faaa! = Long time ago in a galaxy not far away at all!
uTVM,TPw55:utvm,tpwstillsecure = Until this very moment, these passwords were still secure

Natuurlijk moet je geen van de bovenstaande voorbeelden gebruiken, want nu ze als voorbeeld zijn gegeven, zijn ze niet meer geschikt als optie voor een sterk wachtwoord.

Als je gedwongen wordt een wachtwoord te geven
Laten we hopen dat je nooit in de situatie terechtkomt dat je gedwongen wordt om je wachtwoord te verstrekken. Maar, stel dat een kwaadwillende groep of dienst je heeft betrapt met een versleutelde USB-stick (met je belangrijkste bestanden of brondocumenten) en ze zijn bereid om het uiterste te doen om het wachtwoord te verkrijgen om je bestanden te kunnen ontsleutelen. Wat moet je dan doen?

In zo'n situatie kan het helpen dat je een verborgen volume op de USB-stick hebt. Dit volume is niet zichtbaar en lijkt ook geen ruimte op de stick in te nemen, waardoor het niet te detecteren is (maar ook gemakkelijk kan worden overschreven). Het zichtbare, versleutelde volume kan als afleiding werken die ontkenning dat er meer is redelijk aannemelijk maakt. In het zichtbare volume kun je bestanden opslaan die een bepaalde mate van beveiliging en versleuteling nodig lijken te hebben en dit volume heeft zijn eigen wachtwoord. Het verborgen volume bevindt zich echter wel, onopgemerkt, binnen het zichtbare volume en het heeft een ander wachtwoord.

Je kunt zo'n verborgen volume maken met VeraCrypt (zie hoofdstuk 4). Deze methode met het gebruik van een verborgen volume kan helpen om de belangrijkste informatie te beveiligen tegen onderschepping, maar niet tegen verlies. Het volume kan gemakkelijk worden vernietigd of overschreven, dus je moet altijd zorgen voor een back-up van belangrijke bestanden.

Veel van dit hoofdstuk is overgenomen van Bruce Schneier's blog, https://www.schneier.com/. We bedanken de heer Schneier hartelijk voor de toestemming om zijn suggesties hier over te nemen.

Verklarende woordenlijst

Begrip	Definitie
AMT-chipset	Chipset met 'Intel Active Management Technology' (AMT) voor geautomatiseerd management (kwetsbaarder dan oudere chipsets van voor 2008)
Airgapped	de situatie dat een laptop nooit online gaat (dat geldt zowel voor lokale netwerken als internet) als beveiligingsmaatregel
Backdoor	verborgen kwetsbaarheden in veiligheid die toestaan dat bekende beveiligingsmechanismes van een systeem worden gebypasst, zodat niet te detecteren toegang tot de computer of computerdata mogelijk wordt
Besturingssysteem	de software die de computer bestuurt als deze opstart, vertelt wat er moet gebeuren en hoe dat moet worden gedaan. Het is de basisinterface van de computer, waarmee je met computer kunt werken
BIOS	"Basic Input/Output System" – basis input/output-systeem. Een set computerinstructies in firmware die de input en outputactiviteiten beheert
Bridges (bruggen) Tor	bridges zijn Tor-relays die helpen censuur (blokkades) te omzeilen zodat je toch online kunt gaan met de Tor-browser
Dragnet (sleepnet)	een massasurveillance-systeem dat via programma's data over de hele wereld doorneemt en verzamelt (zowel onlinedata als data van telecommunicatie)
Faraday-kooi/-tas	een metalen omhulsel dat ervoor zorgt dat er geen elektromagnetische velden kunnen doordringen in of kunnen ontsnappen uit het omhulsel
Firmware	op hardware geprogrammeerde software die instructies geeft aan hoe het betreffende apparaat moet communiceren met de andere hardware van de computer (inclusief de BIOS)
Hardware	de fysieke componenten die samen het computersysteem vormen
Malware	kwaadaardige software, bijvoorbeeld spyware, ervoor bedoeld om een computersysteem te verstoren of beschadigen
Man-in-the-middle-aanval	de heimelijke interceptie van communicatie waarbij een tussen-persoon zich gedraagt als doel/ontvanger/contactpersoon
Metadata	data over data
Middleware	programma's die twee verschillende, vaak al bestaande programma's laat samenwerken c.q. lijmt; het maakt databases toegankelijk voor programma's
Node	een computer uit het Tor-netwerk die verkeer doorgeeft aan een andere computer/node
Opensource	gratis gedistribueerde software waarvan de broncode publiek beschikbaar is
Tor-netwerk	een wereldwijd netwerk van computers die Tor-nodes worden genoemd
Tor-relay	nodes of computertoegangspunten die verkeer van het Tor-netwerk ontvangen en dat doorgeven

Over de auteurs

Silkie Carlo is een journalist en activist. Ze werkt vanuit Londen. Ze is afgestudeerd in politiek, psychologie en sociologie aan de University of Cambridge in 2012. Hier voerde ze onderzoek uit naar de mogelijkheden van een omgekeerd justitieel systeem, hierdoor gestimuleerd door het gebruik van WikiLeaks. Silkie werkte met klokkenluiders van inlichtingendiensten en schreef stukken over klokkenluiders voor VICE. Met enige regelmaat geeft ze sociale wetenschappen naast haar werk rondom informatiebeveiliging.

Arjen Kamphuis is co-founder en Chief Technology Officer van Gendo sinds 2005 (http://www.gendo.ch/en/blog/arjen). Daarvoor werkte hij voor IBM as IT-architect, trainer en IT-strategie-adviseur. Hij is sinds 2016 lead-advisor information security bij Brunel. Als CTO van Gendo adviseert hij verschillende nationale overheden, non-profitorganisaties en Fortune-500 bedrijven over hun technologiebeleid. Sinds 2009 traint Arjen journalisten, politici, advocaten, mensenrechten-activisten en klokkenluiders om hun communicatie en data te beschermen tegen inbreuk of manipulatie door bijvoorbeeld overheden en grote bedrijven.

Dit handboek is beschikbaar in o.a. de Engelse, Spaanse en Turkse taal. De Nederlandse vertaling is verzorgd door Helma de Boer van Artheos (www.artheos.nl). Je eventuele feedback op dit boek is van harte welkom. Stuur daarvoor een e-mail aan: helma@artheos.nl (PGP-sleutel 0xEEA94382). Je kunt dit adres ook gebruik voor technische vragen en advies.

Commissioned by the Centre for Investigative Journalism. Creative Commons Licence. (CC BY-NCSA 4.0). Licence for humans. Licence for lawyers.
Information Security