Veilig emailen

Ondanks de snelgroeiende populariteit van internet-berichtendiensten als WhatsApp of Telegram – de eerste heeft nu 1 miljard actieve gebruikers per maand, de tweede claimt er 100 miljoen – is emailen nog steeds de meest wijdverspreide manier van communiceren. Afgezien van praten met je huisgenoten of buren natuurlijk. Wereldwijd zijn er vandaag 2.6 miljard email-gebruikers. Een enorme berg informatie wordt dagelijks verspreid via email en we dragen er allemaal aan bij. Maar is het veilig?

De onthullingen van Edward Snowden hebben definitief het hoofdstuk 'Ik heb niets te verbergen' afgesloten. Spionerende overheden kunnen altijd wel iets vinden dat je bij nader inzien toch liever niet gedeeld had. Maar minstens even groot is het risico van het grenzeloos data verzamelen, zoals vooral grote bedrijven als Google, Facebook, Apple of Microsoft het doen. En verder doet vrijwel alles en iedereen die aan het internet verbonden zijn het: data verzamelen. Ik houd zelf ook een oogje op wie mijn website bezoeken. Het verschil is alleen dat overheden en bedrijven de middelen hebben om die data vervolgens uitvoerig te combineren en analyseren. En vooral ook: te verhandelen. Onderschat ook niet de kans dat overheden en bedrijven hierin eendrachtig samenwerken. Hoe kunnen we tenminste onze email nu afschermen van al deze spiedende ogen?

In Nederland lijkt bijna niemand zich daar druk om te maken, hoewel ons aller AIVD aantoonbaar een van de trouwste hulpjes is van Amerikaanse overheidsdiensten. Òf Nederlanders zijn gewoon goed van vertrouwen, òf ze zijn gevaarlijk zorgeloos. We zien onszelf graag als vrij en eigenzinnig, maar in feite zijn we nogal braaf en gezagsgetrouw. Dat verwijten we liefst onze oosterburen, maar het was een Duitse vriend die mij als eerste om mijn PGP-sleutel vroeg. De Duitsers hebben namelijk goede redenen, uit het recente en minder recente verleden, om zich veel meer zorgen te maken over spionage en privacy. Zij doen binnen de open-source community, maar zelfs van overheidswege al heel veel voor veilige online-communicatie.

Dus heb ik nu **encryptie** opgezet voor mijn email, zodat ik desgewenst mijn berichten versleuteld kan versturen. Uiteraard werk ik alleen op Linux-systemen, met Android als de verstgaande afwijking. Op dit moment is dat LinuxMint met een KDE desktop-omgeving en KMail als email-toepassing. Maar het meeste werk dat ik verderop beschrijf kan op elke Linux-distributie gewoon vanaf de commandline worden gedaan. Eerst wil ik uitleggen wat mijn overwegingen waren en dan hoe ik het heb opgezet. Het is een beetje werk, maar daarna draait alles bijna vanzelf. Maar geloof mij niet op mijn woord: Carla Schroder heeft hetzelfde al glashelder gezegd op Linux.com.

> ***OPMERKING*** *(voor arme zielen die nog aan Windows vastzitten): Gpg4win is waarschijnlijk een goed startpunt. Oorspronkelijk ontwikkeld door het Duitse Bundesamt für Sicherheit in der Informationstechnik, op het Linuxplatform van hun overheidsservers, maar daarna netjes geport naar Windows. Bovendien open-source & gratis. Deze HowTo helpt je op weg.*

Inhoud :

> ***OPMERKING 2****: wie al snapt wat de risico's zijn en al weet waarom encryptie nodig is, kan de eerste twee paragrafen overslaan en meteen doorgaan naar* ***PGP opzetten****.*

De risico's

Het eerste risico is: **spiedende ogen**. Vergeet om te beginnen niet de voordehand liggende zaken: iemand die meeleest op je beeldscherm, iemand die bij je computer kan komen terwijl je wegbent. En zo zijn er meer: per ongeluk een email naar de verkeerde persoon sturen, het ongemerkt doorsturen van jouw email door een ontvanger.

Een steeds serieuzer risico is de mogelijkheid dat je **computer wordt gehackt**. Niet noodzakelijk door criminelen. De Nederlandse overheid wil de politie hackbevoegdheid geven en trekt zich niets aan van de breed geuite bezwaren. Ook onze Amerikaanse vrienden liggen op eenzelfde ramkoers.

Zulke bevoegdheden leiden bijvoorbeeld tot het installeren van een keylogger, alsmede trucs om onzichtbaar te blijven op je computer. Trojans, stealth, phishing – het mag straks allemaal gebruikt worden tegen burgers zonder dat die dat weten. En als de politie het eenmaal mag, waarom dan niet ook de belastingdienst, de gemeente, de (zorg)verzekeraar, de woningbouwvereniging enz. want die bestrijden toch ook allemaal 'fraude'?

In principe moet een goed geconfigureerde Linux-computer hier redelijk tegen bestand zijn. Een indringer krijgt niet zomaar de root-rechten die nodig zijn voor schadelijke acties en een firewall draait meteen op kernel-niveau. Virussen zijn erg zeldzaam en nauwelijks effectief. De kernel en de belangrijkste toepassingen worden zeer geregeld bijgewerkt en wanneer ergens een veiligheidslek wordt gevonden, reageert de Linux community daar doorgaans zeer snel op. Maar ook je Linux-box is geen Fort Knox. En de zwakste schakel is altijd weer de gebruiker: jijzelf dus. (Dat heet onder sysadmins 'PICNIC' = 'Problem In Chair, Not In Computer'.)

Terzijde: opvallend dat Windows 10-gebruikers Microsoft nu al toestaan om te loggen wat ze typen, officieel om de Cortana personal assistant te ondersteunen… Lees dit onthullende citaat uit de EULA maar eens (waarmee je verplicht accoord gaat):

> *We will access, disclose and preserve personal data, including your content (such as the content of your emails, other private communications or files in private folders), when we have a good faith belief that doing so is necessary to protect our customers or enforce the terms governing the use of the services.*

Het is in werkelijkheid de *gebruiker* die wel een heleboel 'goed vertrouwen' moet hebben! Zie ook de concretere uitleg van de How-To Geek.

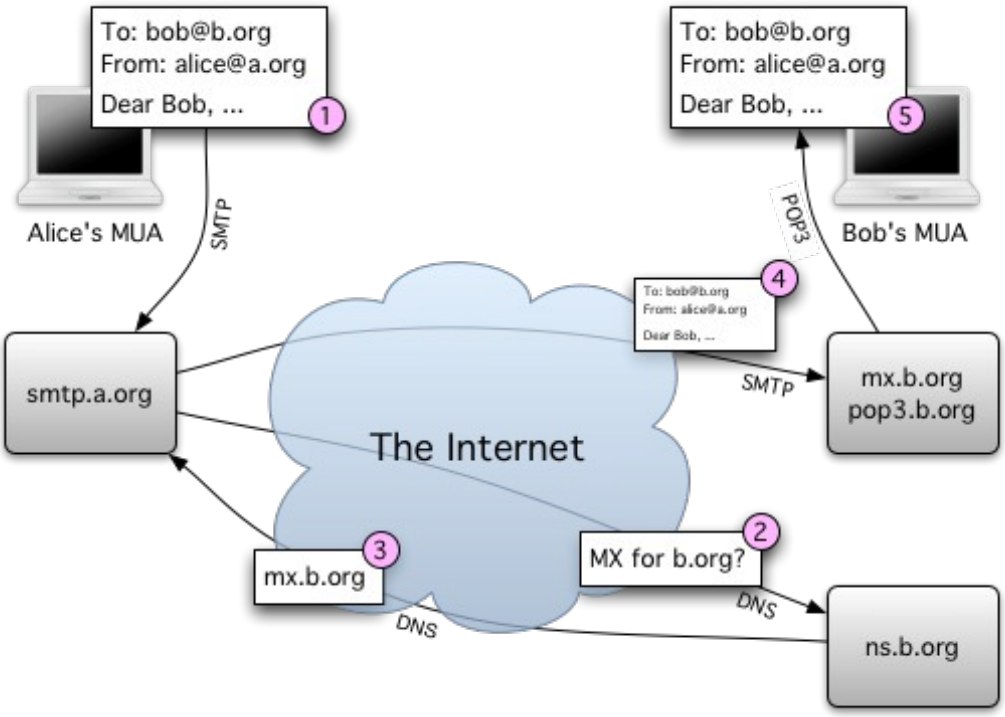
Al genoemd is het risico van **phishing**. Iemand belt of emailt met een schijnbaar legitiem verhaal en dan blijk je je login-gegevens voor je email of een web-account te moeten geven. Nooit doen dus! Ook een argeloze klik op een valselijk geprepareerde weblink kan je al bij zo'n phishing-poging brengen. Altijd opletten waar je heen surft! En het zijn niet eens de minsten die erin trappen…

Email is uiteraard maar een onderdeel van dit alles. Maar omdat alle elementen zo sterk met elkaar verweven zijn, is veilig emailen op zich al een belangrijke stap in de goede richting. Wat email aantrekkelijk maakt voor zowel boeven als 'big brothers', is, dat de herkomst van een bericht en de identiteit van verzender en ontvanger eenvoudig en met redelijke zekerheid achterhaald kunnen worden.

Goed, **wat gebeurt er op je computer en daarbuiten wanneer je emails verzendt of ontvangt?** Laten we eens kijken.

Bij verzenden zoekt je email-programma, via het besturingssysteem, contact met de mailserver van je email-provider (gewoon volgens het TCP/IP-protocol). Die mailserver zoekt op waar de

mailserver van de ontvanger zich bevindt (via een DNS-server) en stuurt het bericht dan door het doolhof van internet daarnaartoe, waarvandaan het dan weer kan worden binnengehaald door de geadresseerde. Dat ziet er ongeveer zo uit:



Er zijn globaal twee methoden van emailverkeer.

Bij de eerste verwijdert de mailserver een bericht van de server zodra het door de ontvanger is binnengehaald op diens compter. Emails worden dan uitsluitend bewaard op de computers van zenders en ontvangers. Dit verkeer wordt geregeld met protocollen voor verzenden (SMTP) en ontvangen (POP3) en daaraan kun je zelf een paar dingen instellen. Dit is de meest gebruikelijke methode voor internet-providers (lees: je kabelaar, KPN, Tele2, XS4ALL, Ziggo enz.).

Bij de tweede methode blijft alle email altijd bewaard op de mailserver, of tegenwoordig meestal 'in de cloud'. Wat verzender en ontvanger op hun computers zien zijn kopieën van de berichten op die mailserver. Dit heet **webmail** en je benadert die dan ook via je webbrowser. Dit is de methode van populaire 'gratis' diensten als Hotmail, Outlook.com, Yahoo! Mail of Gmail. Om het iets ingewikkelder te maken bieden internet-providers zelf meestal ook 'webmail' aan als een extra service. Uiteraard laat die dan alleen de berichten zien die nog niet via het POP/SMTP protocol van de server afgehaald zijn.

Voor wie daarvoor de technische kennis en de middelen heeft is het zeker niet onmogelijk ergens op de route tussen verzender en ontvanger **een emailbericht te onderscheppen**. En voor webmail-diensten is dat risico nog hoger, omdat kwaadwillenden geen toegang tot alle afzonderlijke computers nodig hebben, maar zich gewoon kunnen richten op de mailservers. Aan een achteloos rondslingerend emailadres en wachtwoord hebben ze genoeg om bij de email te kunnen komen. Eigenlijk is een email-adres al voldoende, want (te) veel mensen gebruiken zo'n zwak wachtwoord dat het in een mum te kraken valt.

Om berichten te kunnen verzenden en ontvangen moeten mailservers weten waar het vandaan komt en waar het naar toe moet. Onderweg wordt daaraan toegevoegd langs welke mailservers en internetknooppunten het bericht heeft gereisd. Die gegevens kun je ook terugzien in de 'headers' (of 'kopteksten') van een bericht. Dit zijn de zg. **metadata**. In principe worden die data versleuteld

verstuurd (volgens de regels van het SSL/TLS-protocol), maar bij iedere tussenstap op de route moeten servers natuurlijk wel kunnen lezen wat erin staat om te weten wat ze met de verzonden data moeten doen. En daar zit dan ook de zwakke plek. Alle 'gratis' webmail-diensten houden die metadata uitvoerig bij, analyseren die en verkopen het, vooral aan adverteerders. En de overheid is ook steeds meer geïnteresseerd in deze informatie. Het verhaal van Big Data begint gewoon bij metadata. Als gebruiker is het onmogelijk om te weten wie welke gegevens van jou opslaat en wat daar vervolgens allemaal mee gebeurt.

De inhoud zelf van je email, en de eventuele bijlagen, worden standaard *niet* versleuteld, tenzij je dat zelf regelt. Wie de metadata kan lezen, kan ook de inhoud zien. De koppeling tussen jouw identiteit en jouw inhoud is dus glashelder en die is in de informatietijd inmiddels goud waard. Natuurlijk zitten er geen mensen jouw mail te lezen, maar bots doen dat de klok rond. En dat bovendien stukken sneller, nauwkeuriger en betrouwbaarder dan mensen.

Standaardreactie is nog steeds: 'Maar ik heb niets te verbergen.' Dat is een gevaarlijk misverstand. Want dat emailtje is maar een van de talloze digitale sporen die wij dagelijks achterlaten: zoekgeschiedenis, favorieten, downloads, aankopen, bankverkeer, forum-activiteiten, sociale media, blogs, eigen websites, foto's, video's, cloudopslag, enz. Nog afgezien van wat anderen, vaak ongemerkt, ook al van ons vastleggen: bewakingscamera's, nummerplaatherkenning, gezichts- en stemherkenning, parkeren, huren, vakantieboekingen, pinautomaten, enz. Door al die data te combineren wordt van ieder van ons **een profiel** gemaakt, een verbijsterend gedetailleerd beeld van wie wij zijn en wat wij doen. Zo worden voortdurend onze complete sociale netwerken, onze dagelijkse activiteiten, meningen, politieke overtuigingen, stemmingen, onze gezondheid, religie, ziekten enz. verzameld, geanalyseerd en vooral verhandeld. Met als enig doel ons op grond daarvan te manipuleren, hetzij als consument, hetzij als burger.

De nieuwste trend heet 'slim': slimme meters, slimme apparaten. Maar voor wie zijn die het slimst: voor de gebruiker ('het is zo gemakkelijk') of voor de leverancier die al die verzonden data ook precies kan volgen en verkopen? Alles met een simpele RFID-chip erin kan nu verbonden worden met internet (het 'internet of things') en een gigantische extra stroom data wordt zo geproduceerd. Het is vrijwel onmogelijk nog een plek in de bewoonde wereld te vinden zonder internetbereik (een zg. 'white spot'). Voor alles op internet dat je 'gratis' krijgt betaal je dus met je data.

De risico's afdichten

Terug naar de email. Hoe kunnen we die beveiligen?

Om bij het begin te beginnen: eerst je computer zelf. Denk na als je emailt, aan wie je iets stuurt en wat ermee kan gebeuren als dat doorgestuurd zou worden. Als het niet versleuteld is, wees je dan bewust van wat je schrijft of als bijlage verstuurt. RKHunter zou je kunnen waarschuwen als er op je computer iets ongevraagd wordt uitgevoerd. (Onder Windows hebben veel virusscanners een soortgelijke rootkit-detectie ingebouwd.) Je firewall netjes configureren voor uitgaand verkeer is een andere veiligheidsmaatregel. Maar als een expert je systeem echt wil hacken, is het moeilijk om dat (tijdig) te signaleren of te voorkomen. Surfend op het internet moet je uiteraard niet zomaar op elke link klikken. Browsers als Firefox hebben diverse hulpmiddelen, ingebouwd of als add-on, om je te waarschuwen voor verdachte websites, om cookies en javascript te beveiligen enz.

Voor het verzenden en ontvangen zelf van je email is er al het een en ander aan beveiliging standaard aanwezig. Om met de mailserver van je provider te communiceren wordt het SSL/TLS-protocol gebruikt waarmee je logingegevens versleuteld worden tussen je computer en de mailserver. Maar de inhoud van je bericht blijft nog steeds gewoon leesbaar.

Om die inhoud af te schermen voor spiedende ogen of slimme bots moet je het bericht versleutelen. Het standaardprotocol daarvoor is PGP, tegenwoordig beschikbaar in de vorm van

Open PGP, en in de Linux-wereld is de GNU Privacy Guard (ofwel GnuPG resp. GPG) de meest gebruikte software om dit protocol toe te passen. GPG is een commandline-toepassing. Als je beter wilt begrijpen wat encryptie precies is en hoe het werkt, kijk dan in Wikipedia bij encryptie en cryptografie.

Om het eenvoudiger te maken zijn er GUI-toepassingen rond GPG gebouwd waarmee encryptiesleutels, certificaten en digitale handtekeningen beheerd kunnen worden, bv. Kleopatra, KGpg, Seahorse of GPA.

Alle gangbare emailtoepassingen – Evolution, KMail. Claws Mail, Mutt enz. – kunnen zelf al met GPG overweg. Thunderbird, de cross-platform emailtoepassing van Mozilla, heeft een plugin die versleutelen mogelijk maakt, nl. Enigmail.

Wat betreft webmail: tenzij je dat draait op je eigen domein en met een correct geconfigureerde mailserver, zullen de berichten normaal gesproken niet versleuteld zijn. En zelfs als een provider dat wel doet, heeft die nog steeds zelf de encryptiesleutel, zodat jouw berichten altijd leesbaar te maken zijn (zelfs zonder dat je dat weet). Bovendien is datamining de kern van het verdienmodel waarop deze emaildiensten zijn gebaseerd. Het kost je geen geld, maar je betaalt met je data. Derhalve: wil je het veilig houden, dan vermijd je Gmail, Outlook.com, Hotmail, Yahoo! Mail en consorten.

Het Zwitserse ProtonMail kan een alternatief zijn, omdat deze kant-en-klare webmaildienst altijd alles versleutelt en de gebruiker zelf daarvoor de sleutel(s) heeft. ProtonMail houdt, tamelijk uitzonderlijk, geen logboeken bij van gebruikersactiviteiten. Ook een handige mogelijkheid om vanaf je smartphone of tablet veilig te emailen. Want op mobiele apparaten kijken Apple, Microsoft en Google wel altijd mee bij alles wat je doet.

Maar uiteraard is webmail erg handig omdat je vanaf verschillende plekken, en vooral ook mobiel, bij je email kunt komen. Daarvoor zijn er ook wel veilige, zelfs Nederlandse, diensten, maar dat is meer iets voor bedrijven. Bits of Freedom helpt je op weg als je een alternatief zoekt voor Gmail. Mocht je je eigen webmail op willen zetten: ook de webmailinterface SquirrelMail kan, met een plugin, berichten versleutelen. (Voor Roundcube zit dat nog in de pijplijn.) Daarvoor moet je dan wel een eigen domeinnaam en webhosting hebben, bij voorkeur een VPS, waarop je dan zelf helemaal alles installeert en dus ook zelf de baas bent. Er zijn vele aanbieders. TransIP is een van de Nederlandse die uitstekende diensten biedt.

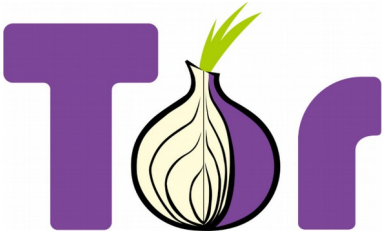
Wanneer je hebt gecontroleerd of SSL/TLS correct is ingesteld en je je emailprogramma hebt geconfigureerd voor encryptie, dan verzend en ontvang je email op een veilige manier. Alleen jij en de ontvanger kunnen een bericht lezen, mits je beiden de betreffende publieke encryptiesleutel hebt. Niet dat dit systeem absoluut onbreekbaar is, maar normaliter zou dit voldoende moeten zijn.

Samenvattend:

- denk na bij wat je emailt en naar wie;
- check op rootkits als je vreest dat er iets raars gebeurt op je computer;
- configureer je firewall voor uitgaand verkeer;
- controleer of SSL/TLS correct wordt gebruikt;
- gebruik OpenPGP voor het versleutelen van je berichten;
- en vermijd 'gratis' webmaildiensten.

Toch kan het nog veiliger. Want ook met versleuteling is nog steeds na te gaan waar een bericht vandaan komt en aan wie het is gericht. IP- en emailadressen en meer details blijven zichtbaar.

Het is niet al te moeilijk om die gegevens te koppelen aan jou als persoon. Dat kun je ook zelf eens proberen. Mailservers houden (wettelijk verplicht) logboeken bij van verzonden en ontvangen berichten. In Nederland moeten die geruime tijd bewaard worden voor het geval politie of inlichtingendienst die zouden willen inzien.



Wil je 'onzichtbaar' over het internet reizen, dan zou je kunnen verbinden via een Tor-netwerk. De verbinding wordt er wat trager van en het duurt ook even voor je verbinding hebt, maar dan is het verder tamelijk makkelijk in het normale gebruik. Zie ook de Tor Project-website voor uitvoerige details. Ook je emailprogramma zal wat nadere configuratie nodig hebben. En voor de nieuwsgierigen: Tor is oorspronkelijk bedacht door de Amerikaanse marine…

Maar wie echt het beste wil voor veiligheid en anonimiteit, zou niet eens vanaf de eigen computer moeten werken, omdat die altijd herleidbare sporen achterlaat. Ook Tor-netwerken kunnen dat niet volledig verbergen. Daar zijn nog extra maatregelen voor nodig en die zijn allemaal al verwerkt in Tails ('The Amnesic Incognito Live System'), een compleet Linux-systeem dat helemaal draait vanaf een USB-stick. Je start je computer vanaf die stick (waarvoor je mogelijk even je BIOS-instellingen moet aanpassen). Het heeft een eigen emailprogramma, Claws Mail, en je kunt je mail versleuteld bewaren op die USB-stick. Het gebruik van Tails was voor journalist Glenn Greenwald en documentairemaakster Laura Poitras een vereiste om veilig in contact te kunnen (of beter: mogen) komen met Edward Snowden.

PGP opzetten

Goed, nu eerst PGP maar eens opzetten. Voor Ubuntu-gebruikers wordt de procedure in detail uitgelegd in de Ubuntu-documentatie. Ik vat samen.

Je kunt het doen met een grafische toepassing als KGpg, Seahorse of GPA, maar het kan ook gewoon vanaf de commandline. Dat werkt altijd.

> ***OPMERKING*** *voor wie KGpg wil gebruiken. Dat installeer je gewoon uit de Ubuntu repositories, maar er zit een bug in het standaard geïnstalleerde bestand* `kgpgrc`*, waardoor het programma de eerste keer niet wil starten. Moet je even handmatig oplossen:*
> - *zoek het bestand* `kgpgrc` *op; bij mij staat het in* `/usr/share/mintkde-default-settings/kde4-profile/default/share/config/`
> - *open het bestand in een terminal met* `sudo nano [volledig-pad]/kgpgrc` *en zorg dat in de sectie* `[GPG Settings]` *deze regel er precies zo in staat:* `gpg_config_path=$HOME/.gnupg/gpg.conf`
> - *opslaan en KGpg start gewoon*

Goed, dan nu de 'terminal way'. Open een terminal om een **gpg key aan te maken**. (Een pgp key is hetzelfde, maar omdat we hier werken met GnuPG, heet het een gpg key.) Dat doe je met het commando:

```
gpg --gen-key
```

Je wordt nu door een paar keuzemenu's geleid. De default keuzes zijn doorgaans wel goed:

```
what kind of key – 'RSA and RSA' voor versleutelen enh digitaal ondertekenen
what keysize     – '2048 bits' is groot genoeg
key is valid for – '0' zorgt dat de sleutel nooit verloopt
```

```
user ID          – '[je-officiële-naam]' bv. zoals op je paspoort
comment          – '[alias of toelichting]' bv. een forumnaam
email address    – '[emailadres]' waarop je werkelijk te bereiken bent
```

Nu type je '0' om de sleutel te laten aanmaken. Er wordt gevraagd om een 'passphrase'. Maak die niet te kort, maar zorg dat je die kunt onthouden. (Schrijf op een briefje dat je ergens VEILIG opbergt.) Het aanmaken duurt een poosje en je wordt gevraagd om willekeurige dingen op je toetsenbord te doen. Als je alles goed gedaan hebt, eindig je met een scherm zoals het volgende:

```
gpg: key D8FC66D2 marked as ultimately trusted
public and secret key created and signed.

pub   1024D/D8FC66D2 2005-09-08
      Key fingerprint = 95BD 8377 2644 DD4F 28B5  2C37 0F6E 4CA6 D8FC
66D2
uid                  David Bowie (Sanger) <david@bowie.net>
sub   2048g/389AA63E 2005-09-08
```

In dit voorbeeld is 'D8FC66D2' de key ID en dat voorbeeld gebruik ik hierna ook. Je vindt jouw eigen sleutel terug in je Home-directory waar die is opgeslagen met een naam als '0xCD8FC66D2.asc'. (De eerste drie tekens horen niet bij de key ID en de extensie uiteraard ook niet.) Sluit de terminal nog niet af.

Om te zorgen dat deze sleutel automatisch gebruikt kan worden door de toepassingen die GPG gebruiken, moet je die **instellen als default** door een regel toe te voegen aan `~/.bash_profile` of `~/.profile` (afhankelijk van je configuratie; de eerste overruled de tweede). Open het bestand in een teksteditor en voeg onderaan een regel als deze toe:

```
export GPGKEY=D8FC66D2
```

Vanaf de volgende login wordt de sleutel nu als standaard ingesteld. Tot slot herstart je de GPG-agent:

```
killall -q gpg-agent
eval $(gpg-agent --daemon)
export GPGKEY=D8FC66D2
```

Als je de sleutel zo hebt aangemaakt dat die nooit verloopt, moet je niet vergeten een '**revocation key**' aan te maken. Daarmee kun je je sleutel herroepen wanneer je die niet langer gebruikt of wanneer een ander die in jouw plaats zou blijken te gebruiken. Of als je je passphrase echt niet meer kunt vinden… Dat doe je zo:

```
gpg --output revoke.asc --gen-revoke D8FC66D2
```

Tenslotte **upload** je je public key naar een keyserver. Je kunt gewoon de Ubuntu keyserver gebruiken uit het voorbeeld. Keyservers wisselen onderling zeer regelmatig public keys uit, zodat jouw sleutel na enige tijd op de meeste keyservers wel gevonden kan worden. Uploaden doe je zo:

```
gpg --send-keys --keyserver keyserver.ubuntu.com D8FC66D2
```

Wil je nog even kijken of je nieuwe (publieke) sleutel inderdaad netjes is toegevoegd aan de keyring op je systeem, dan type je dit:

```
gpg --list-keys
```

Er zou iets als dit op je scherm moeten verschijnen:

```
/home/david/.gnupg/pubring.gpg
------------------------------
pub   2048R/D8FC66D2 2016-01-10
uid                  David Bowie (Sanger) <david@bowie.net>
sub   2048R/389AA63E 2016-01-10
```

Eventuele andere public keys die je op je systeem bewaart zouden daar ook bij vermeld moeten worden.

Als je je public key bijvoorbeeld wilt aanbieden op je eigen website, dan moet je daarvan eerst een zg. '**ASCII-armored version**' maken. Dat doe je zo:

```
gpg --output mykey.asc --export -a D8FC66D2
```

Voor 'mykey' kun je uiteraard de naam invullen die je zelf wilt gebruiken. Deze sleutel vind je ook weer terug in je Home-directory en je kunt die nu uploaden naar je website. Als je het bestand opent in een teksteditor zie je je gpg key als platte tekst. Dat ziet er ongeveer zo uit:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1

mQENBFaL21oBCAD2DCBCWcFc1KG8d0w/lgKQx4xcFwhT9ier7aarT0+qMhzx2d/Y
JOCXyGmwjxsYBLhAbQ7UJrdKe2or/ji8qBwbFM0TPmgoVNKMGEdIG+qNTrk890ND
SWs4MoeGff0RnmzNp3+d5D4k8lcvUBr6XQ45BAbLW36P1lUAsd2eRk9WVRfhBffm
59X6a7KjKcYjKqSkDPlNDoLhEi7lZMiD2k5cP3fBq0eGBecScsLUu6yL3QAPWf1E
YlScKAXdv7wanYGfNhuCJTSVGjuMw4Duk5Wey4JrdkXTIdxm+oPJ3IKve85gLyua
FODhivQ353UjFqce+JX3yKK2EIYdU/9WK7W9ABEBAAG0MU1hcnRpbiBHcmFzaG9m
ZiAoTGludXhSZXYpIDxtYXJ0aW5AbWFybmVsLm9yZy51az6JATgEEwECACIFAlaL
21oCGwMGCwkIBwMCBhUIAgkKCwQWAgMBAh4BAheAAAoJEOLF2Fmx559+XzEH/0gd
HG6N0IgRODrxUXsPZT+ZP7Aq01UIA1bPFDIcCYQ6wPWo0OiYiRaVLxpDz5qrJMuX
QYOgm1jNZg4QWZMrT4meczU2jhFOZamG0aFlFZ8YVWIX7Eox+kBTIU0qikyhmyd/
uyZZzYSjR/INJ84Z7v5NOPzaugyT0vkSqOoA7YawjY3qPMKJcxOFv+1yxhNAPy6Y
Ulc+SttCKKTH/gORrakNdE1CtXLEU8bA8fjBhHSbwUu093hKvB9VTXDd0IxYcuNA
yfRix+xgJtXplfxCRwbN6PM/vW4mtU9JAk/H/tX2xNdDwfsqgGLR36i3bkECw0f4
tsggR7DXYC77yF4e1ge5AQ0EVovbWgEIALg5JbiYtjvagWY5H/pUgBhnxdPNLEpb
FXqQDrr5BHefnDqP8cKQxSVyBfyMObH2pdWcfwLFZ2LnSTu+D3YgY46tsv3mfqcZ
Y09RE0fMgnXeIebGutQPjMZTNwmTddXZZUBXm2p9yo9VhnMUEZWPs+FHCiEbGKpr
S6+CD5V1lcbpEDQba4r106QZkkItnD99Bf9LVy36NwQdWupk73SgU9VUqucVfMvT
/bFRhhO/fX6FgQtFHI+lUUBtVJDOMi+OYfWAgcRftWy25oGf4G8WPSpKir+2OrnT
RPK2X0Y41ej10Vl+dO5/sgwqxnx0N5YuFDu6Yhoq/T9QLsPdsjqa6kcAEQEAAYkB
HwQYAQIACQUCVovbWgIbDAAKCRDixdhZseeffgIACADHGUrMfLUE8pvBW3DhI0g+
oCulh0pF6/oFgg5G/r4NY5ndhUIBxNBRvuTNLdlkDvRtZ9EO7e2x4KCQ3z7WtmaX
BYAsYFQvgqeXDe4TLyEwUW/28fCgx59myTbb12o9X0tmZoIut2R+D8vtLXoero3c
r5wNloNhUp3D5Gv2a+BaSZRQTkHgZPCamhtVLogDpPsSMUZTD+f72FzxbOo07/mS
h/0SOUEdGeLe7cCeSdU2ypyHJqQOCrt5XemrJrpSLufQ2I/1SfA/aowAFEJkyHhJ
2UD2z38lcqvrvhpx+awtLMY+dLxTxhjVzd+pb35UnHuiTxv/uWYIeMqBRc6FyoaL
=IRKz
-----END PGP PUBLIC KEY BLOCK-----
```

Dan de kers op de taart: **maak backups** en bewaar die op een veilige plaats. Eerst je public key:

```
gpg --list-keys
```

Zoek naar de regel die begint met iets als 'pub 2048R/'. Achter de slash staat je key ID. Je exporteert je sleutel als volgt. De naam pas je uiteraard aan:

```
gpg -ao [naam]_public.key --export [key ID]
```

En voor je private key gaat het zo:

```
gpg --list-secret-keys
```

Vind je key ID achter de slash in de regel die begint met iets als 'sec 2048R/' en exporteer die:

```
gpg -ao [naam]_private.key --export-secret-keys [key ID]
```

OK, het was bij elkaar even werk, maar nu is alles helemaal klaar voor gebruik. Je kunt nu de terminal sluiten.

Verplaats de net gemaakte backups van je Home-directory naar een veiliger locatie, bv. een draagbaar medium dat je in een afgesloten kast bewaart. De public key, de revocation key en eventueel de ASCII-armored key kun je verplaatsen naar een veiliger locatie dan je Home-direcory, hoewel de eerste niet echt bewaard hoeft te worden omdat die al is toegevoegd aan de gpg keyring. Je kunt keys veiligheidshalve uitprinten en op dezelfde veilige plaats bewaren, en desgewenst ook je passphrase en fingerprint.

Email opzetten voor encryptie

Nu je je gpg keys hebt aangemaakt, aan je keyring toegevoegd en naar een keyserver geupload, moet je nog even je emailprogramma instellen op het gebruik ervan. De Ubuntu-documentie helpt je weer op weg en ik vat samen.

> ***OPMERKING:*** *de Ubuntu-documentatie is hier en daar wat achterhaald wat betreft de configuratie van emailprogramma's.*

KMail, het standaard emailprogramma van de KDE desktop, heeft alle ondersteuning voor encryptie (PGP/MIME) al ingebouwd. Met dank aan de Duitse overheid die de ontbrekende software liet bouwen en die vervolgens als open-source gratis beschikbaar maakte. Het online handboek legt het hier uit. Samengevat:

- ga naar Settings > Configure KMail > Identities
- kies de identiteit waarbij je encryptie wilt gebruiken
- klik op 'Modify', ga naar de tab 'Cryptography' en klik bij 'OpenPGP signing key' op 'Change'
- voor een emailadres waaraan een gpg key is gekoppeld wordt die key automatisch gevonden
- bij Settings > Composing kun je verder nog zaken instellen

KMail gebruikt Kleopatra als certificate manager en die moet dus wel geïnstalleerd zijn.

Ook **Evolution**, het standaard emailprogramma voor de GNOME desktop (en MATE en, Cinnamon) heeft alle ondersteuning voor encruptie al ingebouwd. Het online handboek legt het allemaal verder uit. Samengevat:

- ga naar Edit > Preferences > Mail Accounts
- kies de mail account waarbij je encryptie wilt gebruiken
- klik op de tab 'Security' en type daar je gpg key ID (zie hiervoor hoe je dat kunt vinden)
- klik op 'OK' en sluit af

Claws Mail heeft een plugin nodig voor OpenPGP-ondersteuning. Ubuntu-gebruikers kunnen die installeren vanuit de gebruikelijke repositories:

```
sudo apt-get install claws-mail-pgpinline
```

De plugin zou automatisch moeten starten en automatisch je gpg keys kunnen vinden. Eventueel moet je de plugin handmatig starten. Ga daarvoor naar Configuration > Plugins. Als een versleuteld bericht geopend moet worden, vraagt Claws Mail om je passphrase. Meer uitleg in het online handboek.

Ook **Thunderbird** heeft een plugin nodig om encryptie mogelijk te maken, nl. de Enigmail plugin. Ubuntu-gebruikers kunnen die installeren vanuit de repositories. Maar het kan ook vanuit Thunderbird zelf, zodat je in elk geval de meest recente versie krijgt. Ga naar het menu Add-ons, zoek op 'enigmail' en installeer de plugin. Bij het herstarten van Thunderbird verschijnt automatisch een venster om Enigmail te configureren. Enigmail stelt een paar vragen en vind automatisch je gpg key. Izza simple! Meer uitleg in het online handboek. En Enigmail heeft ook een eigen online handboek.

Tenslotte **Mutt**, het gouwe ouwe commandline emailprogramma dat al bijna zo oud is als Linux zelf. Ook daarin wordt encryptie prima ondersteund. Je moet het natuurlijk wel zelf in de terminal configureren. Begin bij deze online gids. O, en de humor is inmiddels wat oubollig aan het worden, getuige de slogan van het programma: “All mail clients suck. This one just sucks less.”

Nawoord

Eerlijkheidshalve moet ik toevoegen, dat er voor Gmail wel een hulpmiddel is om berichten te versleutelen met een PGP key: Goopg. Dat is een extensie voor Google's eigen Chromium webbrowser, die overweg kan met de gpg keys op je computer. Je installeert Goopg vanuit een apart toe te voegen PPA repository. Maar ik weet het niet… Het draait op Gmail API's, binnen Chromium. Met andere woorden: het komt allemaal van Gmail zelf en het hoge doel daarvan blijft gewoon datamining. Metadata zijn voor Gmail sowieso toegankelijk.

Mocht je je email helemaal zelf willen opzetten via je eigen VPS (zie ook hiervoor), dan kun je sinds kort gratis certificaten ophalen bij Let's Encrypt. Het project wordt ondersteund door de Linux Foundation en ook gesponsord door serieuze spelers als Mozilla, Cisco en Hewlett Packard. En, ja hoor, ook door Chrome en Facebook…

Marien Grashoff <marien@marnel.org.uk>
mei 2016