18 TIPS VOOR EEN BETERE SECURITY

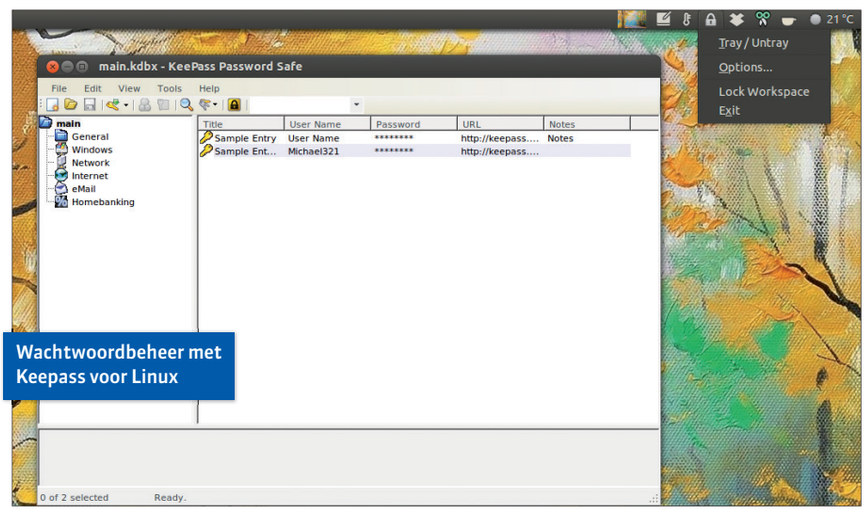
Linux & AVG/GDPR

De AVG-wetgeving is sinds 25 mei 2018 een feit. Deze wet schrijft voor dat je de security op orde moet hebben om de privacy van -naar natuurlijke personen herleidbare- gegevens te waarborgen. Werk je met Linux, dan zit je al op de goede weg. Maar het kan altijd beter en voorkomen is beter dan genezen. Hier een checklist met 18 tips om je Linux-desktop of –laptop nog veiliger én AVG-proof te maken. **Marcel Beelen**

1 Gebruik een **firewall** (veelal **iptables**) en schakel deze ook in als dat niet het geval is. Vind je een firewall configureren lastig, kijk dan eens naar **Gufw**, (**http://gufw.org**) een grafisch front-end voor de firewall en voor de Uncomplicated firewall of gebruik Untangle firewall (**https://www.untangle.com**).

2 Virussen zijn er weinig voor Linux. Een **anti-virus applicatie** kan echter geen kwaad. Kijk eens naar het commandoline georienteerde **ClamAV** (**https://www.clamav.net**) en de grafische schil erbij **ClamTk** (**https://dave-theunsub.github.io/clamtk**). Je zoekt naar rootkits met **rkhunter** (**http://rkhunter.sourceforge.net**) of **ckrootkit** (**http://www.chkrootkit.org**) afhankelijk van je distro). Security auditing doe je met **Lynis** (**https://cisofy.com/lynis**) en extra security op je bestanden voeg je toe met **ESET File Security** (**https://www.eset.com/nl**). Commercieel kan het ook met **Sophos** (**https://www.sophos.com/en-us.aspx**), **FSecure** (**https://www.f-secure.com**), **Avast** (**https://www.avast.com/nl-nl/linux-server-antivirus**) of **Kaspersky** (**https://www.kaspersky.nl**). De tijd dat de commerciële jongens geen Linux ondersteunden, ligt inmiddels ver achter ons.

3 Gebruik een **applicatie sandbox**. Met **Firejail** (**https://firejail.wordpress.com**) voorkom je dat een applicatie de bestanden op je systeem verandert. De applicatie ondersteunt een volledig afgeschermde modus, maar je kunt ook aangeven welke directories en bestanden vanuit een applicatie wel toegankelijk zijn.



Wachtwoordbeheer met Keepass voor Linux

4 Je wachtwoorden schrijf je natuurlijk nooit op. En je gebruikt op alle plekken een complex en ander wachtwoord. Beheer de vele complexe wachtwoorden met een **password manager** als **Keepass** of **KeepassX**. Er zijn tientallen alternatieven te vinden. Stel je Linux systeem zo in dat complexe wachtwoorden verplicht zijn en dat hergebruik van wachtwoorden niet mogelijk is.

5 Maak altijd **back-ups** van je belangrijke bestanden. Gebruik een **NAS** (bijvoorbeeld FreeNAS of een commerciële NAS van een kleine honderd euro) en kopieer periodiek (dagelijks of zelfs continue) gewijzigde bestanden naar de NAS. Dit kan bijvoorbeeld met **rsync**, met eraan toegevoegd het grafische front-end **Grscync**. Ook kun je **Duplicity**, **Duply**, **Duplicati** of **Déjà Dup** gebruiken. Uiteraard beveilig je de NAS met een krachtig wachtwoord.

6 **Versleutel belangrijke bestanden** op je schijf, met bijvoorbeeld **ccrypt**, **keybase** of een compleet virtueel bestandssysteem met **VeraCrypt**. Je kunt zelfs de gehele harde schijf versleutelen als je Linuxdistro dit installeert (het handigste doe je dit tijdens de installatie van het os). Privacygevoelige gegevens op een NAS, zijn eveneens te versleutelen als extra beveiligingslaag.

7 Gebruik **tweeweg authenticatie** daar waar mogelijk. Een extra beveiligingslaag die gebruik maakt van iets wat je “hebt” (zoals een token, smartphone en SMS-bericht) maakt beveiliging een stuk beter. Zelfs ware open source aanhangers en Linux-ge-

bruikers vertrouwen Apple, Google, Microsoft en andere bedrijven op dit vlak en gebruiken en implementeren tweeweg authenticatie van deze aanbieders.

8 **Gebruik geen Windows-applicaties**. Windows-applicaties zijn massaproducten, die sneller bugs bevatten en die voor hackers interessanter zijn om te misbruiken. Als je laptop dual-boot Linux/Windows gebruikt, pas dan op wat je onder Windows doet. Werk liever met een Windows Virtual Machine als je echt Windows-functionaliteit nodig hebt. Windows-applicaties die je draait onder WINE of soortgelijke oplossingen, zorgen ervoor dat je Windows-applicaties onder Linux draait, maar ze zijn in theorie niet in staat de Linux-omgeving in problemen te brengen.

9 **Vergrendel je scherm** als je de werkplek verlaat met de standaard screensaver van Cinnamon, MATE of GNOME. Je kan ook **i3lock** (**https://github.com/i3/i3lock**), **Slock** (**https://tools.suckless.org/slock**) of **XsecureLock** (**https://github.com/google/xsecurelock**) installeren. Het is een kleinigheidje, maar als iemand op het werk langs een PC loopt zonder schermbeveiliging, dan zijn gegevens wel erg gemakkelijk in te zien.

10 **Werk je systeem bij**. Veel distro's werken automatisch de security patches bij. Controleer de update-instellingen van jouw favoriete distro en zorg dat je kleine en grote updates en upgrades (eventueel gepland) ontvangt. Vergeet eveneens niet de packages bij te werken. Merk op dat veel apparaten in huis op Linux draaien. Ook deze dienen periodiek van nieuwe 'firmware' te worden voorzien (denk aan mediaplayers, je router, access points). Zelfs minder voor de hand liggende devices dien je periodiek te upgraden: je printers, je digitale camera's, home automation oplossingen en dergelijk.

11 **Surf veilig**. Controleer of je verbinding maakt met https en **check de security instellingen** in je favoriete browser(s). Voor de meeste browsers bestaan extensies om het werken op internet nog veiliger te maken, denk aan **HTTPS-Everywhere** of **Disconnect**. Schakel het automatisch draaien van scripts standaard uit (bijvoorbeeld JavaScript, Flash).

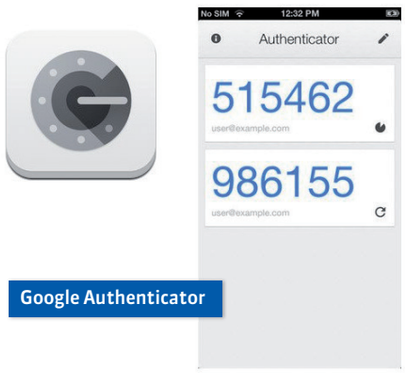
12 Gebruik een **addblocker** als je niet de hele tijd lastig wilt worden gevallen door spam en potentiele malware, bijvoorbeeld **Adblock Plus** (**https://adblockplus.org**). Sta reclame op legitieme sites wel toe, hun bestaansrecht is veelal opgebouwd rondom reclame-inkomsten.

13 Controleer ook de **privacy-instellingen** van je favoriete browsers. Veel informatie hoeft namelijk niet te worden doorgegeven aan de ontwikkelaar als je dat niet wilt. Anoniem zoeken doe je op **duckduckgo.com**. Deze zoekmachine garandeert dat zoekacties niet worden bewaard en dat je privacy gewaarborgd is.

14 Populair zijn tweeweg authenticatiediensten die een sms-bericht sturen naar je iPhone of Android-smartphone. Veel Linux-gebruikers werken met een smartphone met iOS of Android. Omdat dit apparaat misschien nog wel belangrijker is dan je Linux werkplek, is het zaak ook je **mobile device goed te beveiligen**. Als iemand toegang krijgt tot je mobiel, dan hebben deze hackers indirect ook toegang tot sites die beveiligd zijn met tweeweg SMS-authenticatie. Anti-virussoftware, add-blockers of een firewall zijn misschien niet zo relevant, maar back-ups, versleuteling en het bijwerken van je systeem zeker wel! Wat betreft het bijwerken van je device: Apple heeft dit proces sterk onder controle, maar Google een stuk minder. Google smartphones worden slecht bijgewerkt, omdat de fabrikant (Samsung e.d.) dit moet uitvoeren. Wil je een Android device? Kijk eens naar Android One, het door Google onderhouden besturingssysteem voor mobiele devices. Is security en privacy belangrijke voor je, kies dan een smartphone die Android One draait.

15 **Keep it clean**: verwijder ongebruikte applicaties, bloatware en apps, schakel onnodige processen en services uit, verwijder onnodige log- en tijdelijke bestanden. Poets de cache in je browsers eveneens regelmatig. Er bestaan hier gespecialiseerd tools voor, zoals **BleachBit** (**https://www.bleachbit.org**). Minder rommel betekent minder kans op besmetting. Een bijkomend voordeel is dat je systeem sneller opstart en wellicht (een beetje) sneller functioneert.

16 Als het niet noodzakelijk is, **werk niet met publieke WiFi-hotspots**. Gebruik liever de **personal hotspot** op je smartphone om op je Linux-laptop te surfen. Verbind je laptop met WiFi met je smartphone en je smartphone via 4G met internet. Moet je toch met een WiFi hotspot communiceren? **Versleutel communicatie** dan door een VPN-verbinding te gebruiken, bijvoorbeeld met **Open VPN** (**https://openvpn.net**) of **SortEther** (**http://www.softether.org**). Pas op met gratis VPN-diensten, deze zijn niet per definitie veilig. Voor gevorderden: **versleutel je mail** eventueel met **GnuPG** (**https://gnupg.org**).



Google Authenticator

17 Let op je data. Een beetje een open deur, maar toch: deel niets in de social media dat je niet wilt delen. Deel geen informatie over anderen als je daar geen toestemming voor hebt. Teksten en foto's op internet kunnen een eigen leven gaan leiden. Cloud **dataopslagdiensten** zijn overal. Je weet nooit zeker of je data daar veilig is, noch in welk land deze worden bewaard of hoe de beveiliging en privacy zijn geregeld. Om veilig bestanden uit te wisselen, is het slim je eigen cloud te gebruiken, bijvoorbeeld **ownCloud** (**https://owncloud.com**)

18 Misschien wel het allerbelangrijkste: **ken je tools**! De zwakste schakel is toch vaak de mens (de gebruiker van een computer of de beheerder van een systeem of applicatie). Ervan uitgaande dat we geen kwaad in zin hebben: een fout is snel gemaakt. En hoe meer securitymaatregelen we nemen, des te ingewikkelder het werken met de systemen wordt. Security is omgekeerd evenredig met gebruiksgemak. Zonder goede kennis van je tools (besturingssysteem, applicaties, instellingen) en de securitymaatregelen gaat het simpelweg een keer mis.