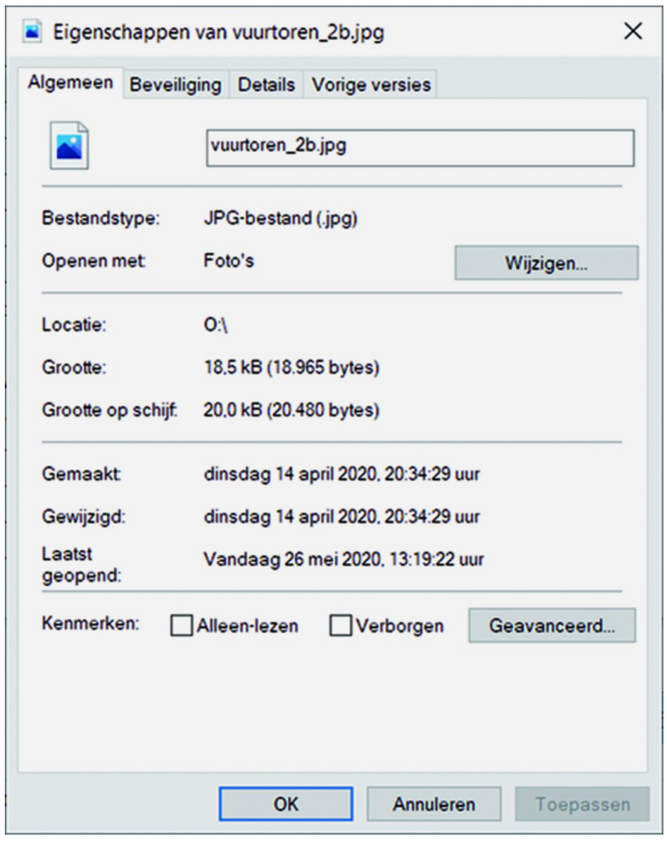
Bestandsbeveiligingen van niks tot beter

Kees van der Vlies

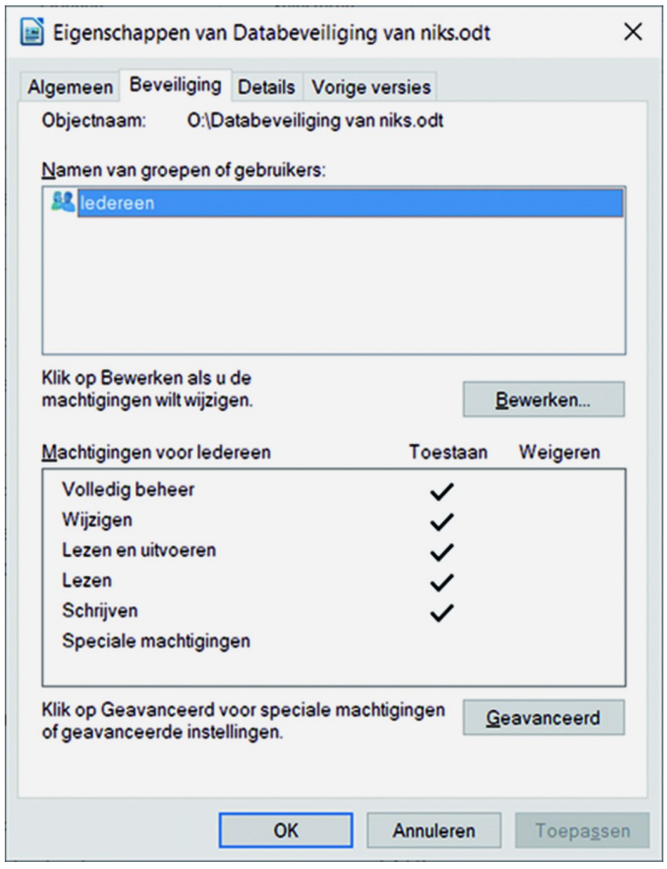
Het beveiligen van computerdata kan op verschillende niveaus gebeuren. U kent allemaal termen als *wachtwoord-(beveiliging), versleuteling (of encryptie), vergrendeling, lees- en schrijfrechten, verificatie, autorisatie (authorization)* en de verschillende procedures en hulpmiddelen: *captcha, calculator-achtige apparaatjes (bij internetbankieren), QR-schermcodes, RFID (draadloos), tweetrapsbeveiliging* (bijv. met een ontsleutelingscode op uw smartphone), beeldscherm-op-zwart en/of hard disk stopt na enige tijd van inactiviteit, vaak bedoeld als energiebesparing. En nog wat andere middelen, zoals vingerafdruk, vingerbeweging op touchscreen, irisscan, gezichtsherkenning, stemherkenning.

Die beveiligingsmiddelen kunnen zeer complex zijn en worden steeds geavanceerder, want de praktijk heeft geleerd dat onverlaten altijd misbruik maken van gaten of achterdeurtjes en vooral van menselijke slordigheid of onoplettendheid.

Wat ik hier ga beschrijven is in de verste verte niet *'de'* oplossing van computerbeveiliging. Integendeel, koester geen illusies v.w.b. de kwaliteit. Het gaat er slechts om dat anderen die even snel een blik willen werpen op uw computer of aangesloten geheugen, daar niet bij de eerste de beste poging in zullen slagen. De beschreven 'trucjes' zijn ook makkelijk toe te voegen aan betere beveiligingsmiddelen. En u weet ook: *een USB-stick kan makkelijk in verkeerde handen terechtkomen!*
De beschreven methoden gedragen zich niet altijd gelijk onder Windows, iOS en Linux. Ik beschrijf de Windows-manier.



*Het tabblad **Algemeen***



*Het tabblad **Beveiliging** - Rechten voor iedereen*

Meer gebruikers op 1 PC

Als u op uw PC meerdere gebruikers(machtigingen) hebt, wordt het iets anders. Dan kan een geautoriseerde gebruiker alleen zijn of haar 'eigen' bestanden zien. Een Beheerder/ Administrator kan wel alles bekijken en heeft veel meer rechten. Maar de meesten onzer zullen slechts één gebruiker op hun machine hebben.

Maak geheugen, bijv. USB-stick onzichtbaar

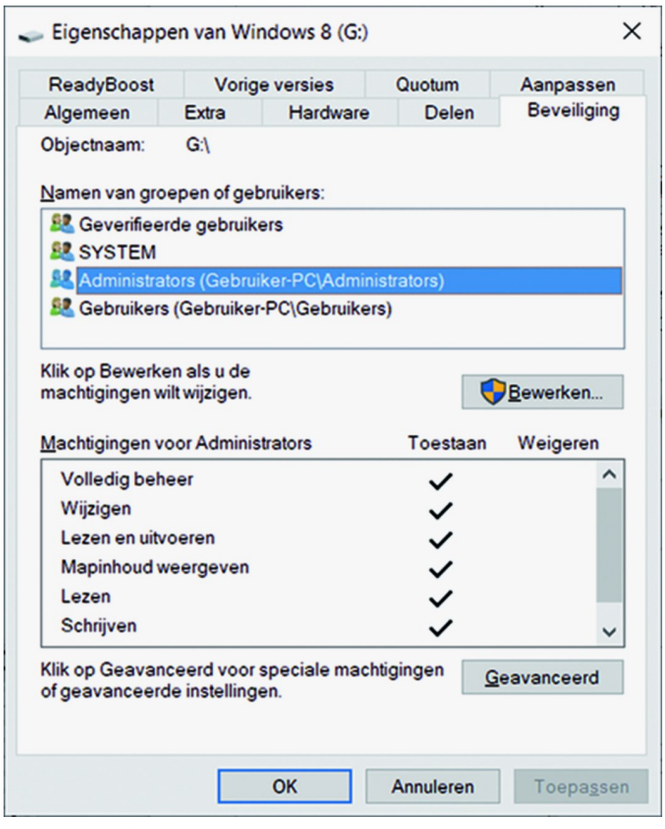
Eerst: bestanden of mappen 'onzichtbaar' of onwisbaar maken.
Elk bestand of map kan het kenmerk 'onzichtbaar' krijgen. Dit is even gemakkelijk te maken als ongedaan te maken.

1. Klik in de Verkenner met de rechtermuisknop op een bestands- of mapnaam en kies voor *Eigenschappen*. Het tabblad *Algemeen* wordt als eerste getoond. Bij het kiezen van een hele schijf ziet het er iets anders uit. Zie de afbeelding .
2. Veranderen gaat dan door het vakje daaronder bij *Kenmerken* het vakje *Verborgen* aan te vinken. U ziet dat Alleen-lezen de andere keus is. Beide aanvinken is ook mogelijk.
3. Dit biedt weinig zekerheid, maar kan een heel kleine drempel bieden tegen een oppervlakkige pottenkijker. Want het tonen van 'verborgen' bestanden is een fluitje van een cent. Misschien hebt u zelfs al 'Verborgen bestan-

den weergeven' standaard aan staan en dan verandert er dus niet veel.

We gaan een stapje verder

4. Na het tabblad Algemeen is het interessant het tabblad *Beveiliging* te openen. U ziet dan eventuele groepen of gebruikers, die op uw pc geregistreerd zijn en daaronder een opsomming van hun machtigingen. Die zijn aan te vinken onder *Toestaan* of onder *Weigeren*.
   Dat gaat dan door eerst op de knop *Bewerken* ... te klikken.
   Bedenk dat u hiermee ook uw andere bestanden kunt behoeden tegen wissen of wijzigen door het vinkje achter *Schrijven* te verhuizen naar de kolom *Weigeren*. Wijzigen van het bestand kan dan nog wel op het scherm, maar

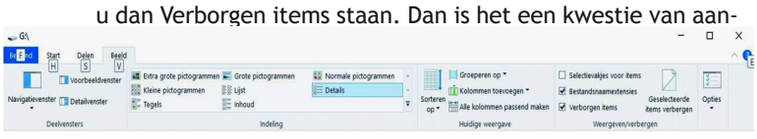


Het tabblad ***Beveiliging*** *- Rechten voor iedere gebruiker of gebruikersgroep individueel instellen*

wegschrijven niet meer. Ook niet onder een andere naam; daar is natuurlijk over nagedacht.

Verborgen bestanden zichtbaar maken

Op schijfniveau zijn 'Verborgen bestanden' of mappen weer te geven of niet - het werd hiervoor al genoemd. Dat gebeurt door in de Verkenner het tabblad Beeld te kiezen. Rechts ziet u dan Verborgen items staan. Dan is het een kwestie van aan-



of uitvinken. Kijk ook rechts daarvan *Geselecteerde item verbergen* voor de mogelijkheden.

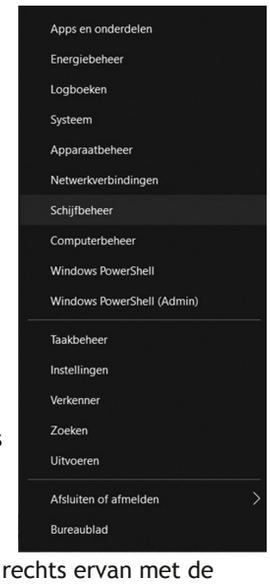
Partitie verbergen

Omdat Windows maar 1 primaire partitie kent, zou u een te verbergen bestand kunnen wegschrijven naar een tweede partitie. Ja, het is een heel gedoe, als u gewend bent alleen onder Windows te werken. Maar als u een beetje overweg kunt met Linux, is het niet zo moeilijk. Een groot nadeel is dat u voor het toegang krijgen tot de partitie wel weer naar Linux moet. U weet toch dat u Linux niet hoeft te installeren op uw pc? Een bootable (life) Linux-distro op een CD/DVD, USB-stick of ander flashgeheugen kan prima gebruikt worden. Dit vereist enige bekendheid met het opstarten vanuit BIOS of (U)EFI. En als u dat dan toch doet, kunt u dit externe geheugenmedium net zo goed meteen gebruiken voor het versleuteld opslaan van uw beveiligde bestanden. Die zijn dan in de meeste gevallen echter niet meer te wijzigen of te wissen. Een uitweg is hier dan in sommige live-versies (m.n. Ubuntu of Ubuntu-derivaten) 'persistentie' op het bootable Linux-medium.
Dan kan er ook nog gewerkt worden met *Volumes* of met *mount points*. Daarvoor zou u met *Windows Disk Management*, *Windows PowerShell* en/of *Diskpart* aan de slag moeten.

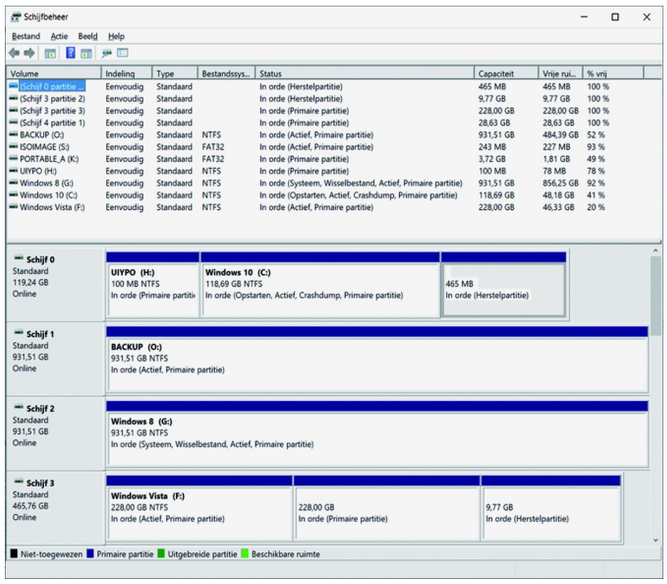
Persoonlijke gegevens verwijderen

Buiten het kader van dit artikel valt het verwijderen van persoonlijke gegevens, zoals die op computers in bestanden en besturingssysteem staan en - niet te vergeten - op talloze servers in het wereldwijde web. Lees daarvoor wat Menno Schoone vermeldt op:
https://www.schoonepc.nl/nieuwsbrief/internet_explorer_privacy_keeper.html

Schijfbeheer gebruiken

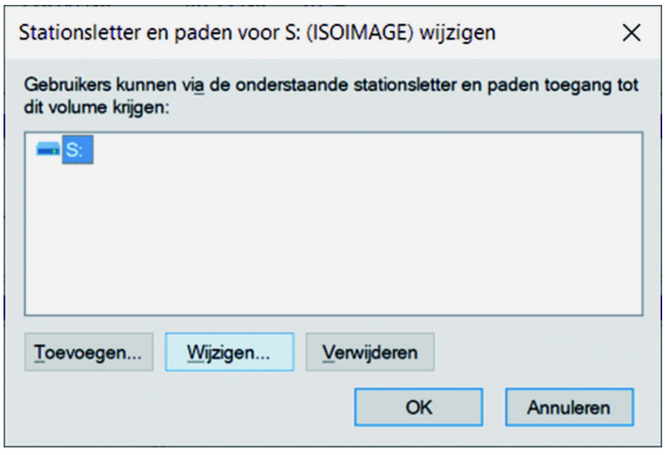


Klik met de rechtermuisknop op het venstersymbooltje geheel links in de werkbalk beneden in het scherm; de zgn. Startknop. In het lijstje ziet u *Schijfbeheer* staan. Als u daarop klikt, wordt de gehele inventarisatie van uw schijven, waaronder ook externe geheugenmedia, zoals USB-sticks, getoond. Eventuele door Windows niet herkende media, zoals schijven met Linux-partitie wil Windows niet zien, ook niet in de Verkenner. Alleen de schijven met FAT, EXFAT en NTFS-formaat worden getoond.
Klik in het vakje Schijf <nr> of in het vak rechts ervan met de rechtermuisknop en er komt een venstertje, waarin u o.a. de schijfletter, die nu ineens Stationsletter heet, kunt wijzigen. U kunt ook op *Verwijderen* klikken.

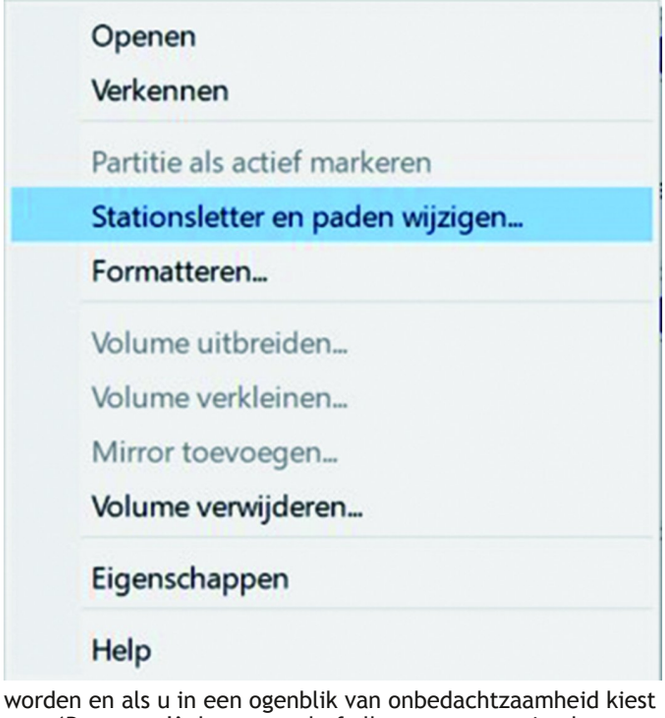


Géén schijfletter toekennen

Als u m.b.v. de Minitool Partition Wizard, EaseUS Partition Master, AOMEI Partition Assistant of een soortgelijke tool



werkt, kunt u de schijfletter van een extern medium wijzigen en kiezen voor *geen schijflettertoekenning*. Dus is dus *niet* een *automatische lettertoekenning*, maar **géén!** Windows heeft het daar moeilijk mee.
Weet wel wat u doet, want op zeker moment kan Windows vinden dat het medium *geformatteerd* of *hersteld* moet



worden en als u in een ogenblik van onbedachtzaamheid kiest voor 'Doe maar!', kan er veel of alles van uw mooie plannetje met een verborgen bestand, map of schijf de mist in gaan.

Letterkleur: wit

U weet misschien dat in tekstbestanden de letterkleur *wit* kan worden gekozen. Ook in een pdf-bestand is dan geen tekst te zien. Maar u moet dan wel onthouden dat er tekst staat, die selecteren en via de letteropmaak weer een zichtbare kleur geven.
En u kunt tekst enz. *afdekken* met een *wit tekstvak*.

Verborgen tekst

Iets anders is het instellen van *Verborgen tekst*, een functie van MS Office en Libre Office, die ook van pas kan komen *bij werkbladen* in spreadsheets.

Bestandsnaam-extensie wijzigen

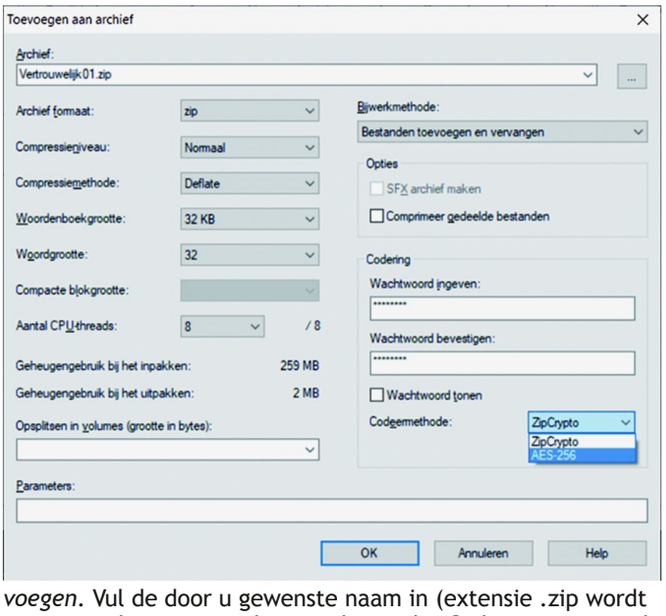
Een andere hindernis die u kunt opwerpen tegen toevallige rondneuzers kan zijn: de bestandsnaam-extensie van een document te wijzigen, bijv. in .txt, .png, .mp3 of een zelfgekozen extensie. Windows zal dan bij een poging het bestand te openen meestal een foutmelding laten zien dat het bestand niet geopend kan worden (met de standaardapplicatie) en u de keuze bieden het met een andere toepassing te proberen. Als u dit doet met een gecodeerde bestandsnaam, valt uit de naam van het bestand ook weinig op te maken.

U weet dat u een bestandsnaam (incl. extensie) kunt wijzigen op twee manieren:
- door met de rechtermuisknop erop te klikken en in het uitrolmenu te kiezen voor naam wijzigen.
- door met ingedrukte linkermuisknop het bestand aangeklikt te houden tot de naam in een blauw vakje weergegeven wordt en u meteen de nieuwe naam (+ extensie) kunt intypen.

Allemaal goed en wel, het legt wel een extra last op u als eigenaar van het bestand. U moet immers later ook nog weten om welk bestand het iedere keer gaat en voordat u er toegang toe kunt krijgen de juiste extensie terugzetten. En zoals veel van de hier genoemde beveiligingsmiddelen zal het voor een beetje computerkenner een kleine moeite zijn er doorheen te komen.

Voor een betere (echte) beveiliging

Versleutelen kan ook met comprimeren samengaan: bekend onder de benaming: zippen. Met 7-Zip gaat dit heel gemakkelijk.
Open het zipprogramma, kies het bestand/de bestanden *toe-*



voegen. Vul de door u gewenste naam in (extensie .zip wordt automatisch toegevoegd) en rechts onder Codering tweemaal het wachtwoord waarmee u het zip-bestand wil versleutelen. Er is keuze uit ZipCrypto of AES-256 wachtwoordcodering. De naam van bestand blijft dan zichtbaar (met de extensie .zip), maar het is zonder wachtwoord niet te openen. Dat kan met hetzelfde programma. Vervolgens zou u de naam wel onzichtbaar kunnen maken.

Versleutelde USB-sticks en extene HD's

Voor het echt serieuze werk zijn USB-geheugenstaafjes met ingebouwde encryptie te koop.
Een paar bekende merken leveren die: SanDisk, ADATA, Kingston/DataTraveler, Verbatim, Imation, Transcend, Lexar, Toshiba.
Maar ook minder bekende namen verschijnen ten tonele: Aegis Secure Key, Workspace, DataLocker. Kanguru/Defender/FlashTrust, XtremKey (van het bekende merk LaCie), Integral, GuardKey, T-KEY, iStorage/datAshur/diskAshur en IronKey.

Voor de versleuteling worden verschillende technieken toegepast: software al dan niet in combinatie met hardware componenten. Sommige modellen hebben zelfs een numeriek toetsenbordje (vrij groot) of een 'biometrische' herkenning: een vingerafdruksensor.
Aan de encryptiekant zien we meestal de door 2 Belgen ontwikkelde AES (Advanced Encryption Standard)-versleuteling (256 bit) voorkomen.

In alle gevallen zijn deze speciale USB-sticks fors duurder dan gewone USB-sticks. Ik kwam prijzen tegen van enkele tientjes tot in de vijf- en zeshonderd Euro.
Ze zijn vaak ook mechanisch veel sterker, in metaal uitgevoerd of waterproof.
Voor smartphones bestaan weer andere modellen.
Ook zijn externe hard disks en SSD's te koop met versleuteling en bijv. een vingerafdruklezer of toetsenbordje op de behuizing.

Op de markt verkrijgbare externe geheugenmedia met stemherkenning of irisscan en -verificatie heb ik niet kunnen vinden. Wel biedt de pc daar mogelijkheden voor, bijv. Gatekeeper van Nuance (technologie van v/h Dragon vv/h Lernaut & Hauspie - weet je nog wel, foutje), een bedrijf dat bijv. ook gespecialiseerd is in beveiligde medische data-uitwisseling. Er is overigens verschil tussen spraakherkenning en stemherkenning. Windows en Google/Android hebben wel spraakherkenning, maar voor stemherkenning gelden andere parameters; immers op elkaar gelijkende stemmen moeten onderscheiden kunnen worden.

Het zal u niet verbazen dat er nog steeds veel te doen is over versleuteling, die door 'bevoegde' overheidsinstanties wel of niet te ontcijferen zou (moeten) zijn.
Nu door de coronamaatregelen steeds meer thuis gewerkt wordt, is bij bedrijven en instellingen de belangstelling voor betrouwbare authenticatie ook flink toegenomen. Veiligheid is toch een eerste vereiste!

Er zijn diverse inpak/uitpakprogramma's, zoals WinRAR, PKzip, Ashampoo ZIP free, RarZilla, PeaZip en jZip die deze mogelijkheid vaak ook bieden.
Wist u dat er ook veel online (gratis) compressieservices zijn:
https://www.wecompress.com/
https://www.youcompress.com/
https://archive.online-convert.com/convert-to-zip e.a.?

Sommige zijn speciaal voor audio-, doc-, video-, jpg- of pdf-bestanden. Zelfs zijn compressiefuncties als *add-ons* van browsers te installeren, bijv. in de Chrome-webstore. Al deze diensten verzekeren dat de hele procedure veilig is.

BitLocker

Microsoft heeft een goede beveiliging van geheugenmedia in het programma BitLocker uitgebracht. Maar BitLocker is alleen in de recente professionele Windows-edities (standaard) beschikbaar. De meeste thuisgebruikers werken met Windows Home. Alle gebeugendragers moeten voor BitLocker speciaal geformatteerd en gepartitioneerd worden.

Andere encryptieprogramma's

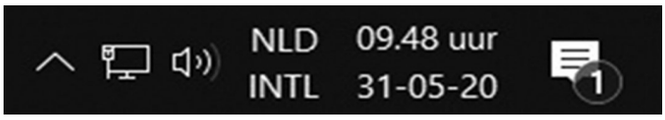
Er zijn betaalde en gratis versleutelingsprogramma's. Zoals:
- VeraCrypt (v/h TrueCrypt) **https://www.veracrypt.fr/en/Home.html** voor Windows, MacOSX en Linux.
- AES crypt (open source, gratis voor Windows en Linux; **https://www.aescrypt.com/**
  lees ook: **https://www.schoonepc.nl/nieuwsbrief/encryptie_bestanden.html**
- AxCrypt
- DiskCryptor
- GNU Privacy Guard
- SecurStick (gratis)
- free Cryptsetup (voor Linux)
- LaCie Private-Public (het staat weliswaar vermeld op de website, maar is het nog te downloaden?)
- **encsecurity (https://www.encsecurity.com** (een Nederlands bedrijf; licenties vanaf 15 Euro eenmalig, gratis proefperiode)
- Ook Norton, McAfee en Kaspersky zijn op de markt met veelzijdige beveiligings- en versleutelingsproducten.

Het gebruik van lange wachtwoorden (met speciale tekens) verkleint het gevaar voor kraken. Acht tekens is inmiddels het (al ris-

kante) minimum. Ga maar boven de 20, als het er echt om spant! Of gebruik een wachtwoordbeheerder die dit voor u opknapt.

Wachtwoordhindernisje met *tweede* toetsenbord

Om nog een kleine extra verwarring toe te voegen voor wachtwoordmisbruikers kunt u een tweede toetsenbordcodering, gebruiken bijv. Nederlands en neem dan in het wachtwoord tekens op die bij US- en Nederlandse toetsenborden niet op dezelfde plaats zitten: ~ & ? : \ ‘] ? + [( ) + = # - ; : ‘ @, mits die tenminste door de wachtwoord-check geaccepteerd worden. De tekens ± ° § staan wel op een Nederlands, maar niet op US-toetsenbord. Maar u kunt natuurlijk nog andere en meer toetsenbordindelingen kiezen. Voor het intypen van het wachtwoord moet dan eerst het andere keyboard gekozen worden. Dit in geval iemand uw wachtwoord heeft achterhaald en het wil gebruiken om in te loggen onder uw naam. Vergeet niet daarna weer terug te schakelen naar uw standaard-toetsenbordindeling (bij ons meestal US alt int). Misschien moeilijk te vinden.
Probeer: *Start* → *Instellingen* → in het zoekvak *Taal* - intypen. In het lijstje eronder verschijnt dan Taal- en toetsenbordopties bewerken. Selecteer eerst onder *Voorkeurstalen* de taal die u al standaard geïnstalleerd hebt. Kies daar *Opties*.



Klik daar op *Een toetsenbord toevoegen* en kies het gewenste toetsenbord.

Soms moet u echter eerst in de pagina *Taalinstellingen* de keuze maken: *Een taal toevoegen*. Of u kunt het met *Geavanceerde toetsenbordinstellingen* proberen

Is het na de zoekpartij allemaal gelukt, dan ziet u rechts onderin het scherm de aanduidingen van de ingestelde toetsenbordtalen verschijnen. Daarop klikken opent de mogelijkheid van overschakelen. Er kan zelfs een sneltoetsencombinatie voor gemaakt worden.

Over de *kwaliteitseisen* van wachtwoorden is al vaak geschreven en gesproken.

Opsplitsen

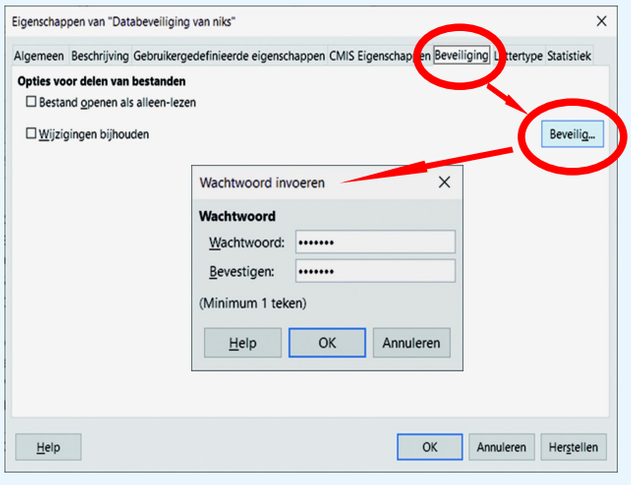
Er zijn methoden waarin u een bestand opsplitst in delen en die apart opslaat, eventueel kunt u die als bijlagen naar uw eigen email-adres sturen of in de cloud opslaan. U zou hier ook eerst (gecodeerde) pdf-bestanden of jpeg-bestanden van kunnen maken. Zet ze niet bij elkaar, dat valt te veel op.
En wederom geldt: u maakt het er voor uzelf niet gemakkelijker op, vooral als u het bestand later nog eens zou willen bewerken.

Vergeet de backup niet!
Bij alles wat u doet met bestanden, thuis, op het werk of waar dan ook, loopt u risico dat een bestand beschadigd raakt of zelfs verloren gaat. Dat risico wordt groter naarmate er meer met een bestand ‘gesold’ wordt, zoals hier beschreven.
MAAK DAAROM VAAK BACKUPS! U verkleint daarmee de kans op onherstelbaar verlies. Ook van bijv. een masterpassword van een wachtwoordbeheerder. Het blijft altijd: risico’s tegen elkaar afwegen en indien mogelijk spreiden.

Bestanden met wachtwoord en/of encryptie opslaan

Bij Libre Office kunt u de gemaakte bestanden via *Opslaan als …* beveiligd opslaan op twee manieren: wachtwoord (alleen de toegang is beveiligd), of met GPG een volledige versleuteling, uiteraard ook met wachtwoord. Het acroniem GPG is een woordspelletje. Sommigen zullen zich **PGP** (Pretty Good Privacy) herinneren, dat - ontwikkeld in 1991 door Philip Zimmermann - vanaf 2010 door Symantec vermarkt werd/wordt onder de latere naam SEMS.

De Open Source-gemeenschap *Free Software Foundation* (GNU) heeft op zeker moment de principes van de versleutelingstechniek overgenomen en heel vindingrijk **G**nu **P**rivacy **G**uard uitgebracht: GPG, ontwikkeld in Java-Script en functioneel gelijk aan Open PGP, dat zich in 1997 als project van het commerciële PGP had afgescheiden.
Parallel aan en soms samenvallend met bestandsencryptie heeft zich ook versleuteling van internetverkeer ontwikkeld.
Via *Bestand* → *Eigenschappen* kunt u in Libre Office per bestand ook allerlei beveiligingsmiddelen toepassen: Alleen-Lezen en Wachtwoord, zie de afbeelding.

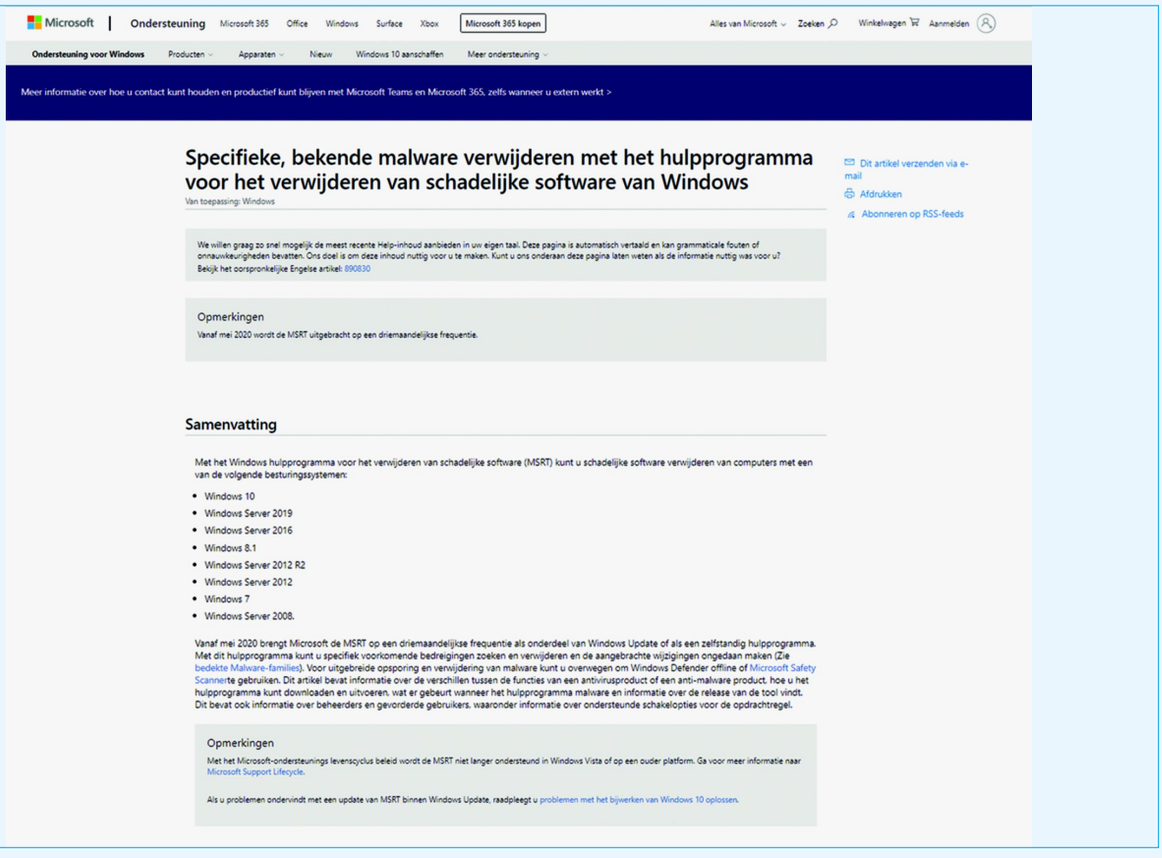


Microsoft Office geeft u eveneens de gelegenheid een bestand met een wachtwoord te beveiligen of alleen toegang geven aan gemachtigden. En ook delen van een bestand kunnen alleen-lezen (dus ook onwisbaar) gemaakt worden. Dit kan bij formulieren of periodieke rapporten handig zijn. De afbeelding toont beveiligd opslaan in Office 2010 en de keuze bij Info. Kijk ook naar de mogelijkheden: Alleen-lezen (Markeren als Definitief), Bewerken beperken en *Een digitale handtekening toevoegen* voor authenticiteit.

Microsoft elimineert malware

Microsoft brengt vanaf mei 2020 MSRT (Malicious Software Removal Tool) elke tweede dinsdag van de maanden februari, mei, augustus en november uit als onderdeel van Windows 10 Update of als een zelfstandig hulpprogramma. Het gaat hier om beveiliging tegen malware en soortgelijke ongein. MSRT schijnt los gebruikt te kunnen/moeten worden naast Windows Defender.

Zie voor nadere informatie en downloads:
https://support.microsoft.com/en-us/help/890830
(Engelstalig).
De software detecteert (gevolgen van) malware op uw computer, rapporteert dit (na uw toestemming) aan Microsoft en meldt u de oplossing.



Microsoft | Ondersteuning Microsoft 365 Office Windows Surface Xbox Microsoft 365 kopen Alles van Microsoft Zoeken Winkelwagen Aanmelden

Ondersteuning voor Windows Producten Apparaten Nieuw Windows 10 aanschaffen Meer ondersteuning

Meer informatie over hoe u contact kunt houden en productief kunt blijven met Microsoft Teams en Microsoft 365, zelfs wanneer u extern werkt >

Specifieke, bekende malware verwijderen met het hulpprogramma voor het verwijderen van schadelijke software van Windows

Van toepassing: Windows

Dit artikel verzenden via e-mail
Afdrukken
Abonneren op RSS-feeds

We willen graag zo snel mogelijk de meest recente Help-inhoud aanbieden in uw eigen taal. Deze pagina is automatisch vertaald en kan grammaticale fouten of onnauwkeurigheden bevatten. Ons doel is om deze inhoud nuttig voor u te maken. Kunt u ons onderaan deze pagina laten weten als de informatie nuttig was voor u?
Bekijk het oorspronkelijke Engelse artikel: 890830

Opmerkingen
Vanaf mei 2020 wordt de MSRT uitgebracht op een driemaandelijkse frequentie.

Samenvatting

Met het Windows hulpprogramma voor het verwijderen van schadelijke software (MSRT) kunt u schadelijke software verwijderen van computers met een van de volgende besturingssystemen:

- Windows 10
- Windows Server 2019
- Windows Server 2016
- Windows 8.1
- Windows Server 2012 R2
- Windows Server 2012
- Windows 7
- Windows Server 2008.

Vanaf mei 2020 brengt Microsoft de MSRT op een driemaandelijkse frequentie als onderdeel van Windows Update of als een zelfstandig hulpprogramma. Met dit hulpprogramma kunt u specifiek voorkomende bedreigingen zoeken en verwijderen en de aangebrachte wijzigingen ongedaan maken (Zie bedekte Malware-families). Voor uitgebreide opsporing en verwijdering van malware kunt u overwegen om Windows Defender offline of Microsoft Safety Scanner te gebruiken. Dit artikel bevat informatie over de verschillen tussen de functies van een antivirusproduct of een anti-malware product, hoe u het hulpprogramma kunt downloaden en uitvoeren, wat er gebeurt wanneer het hulpprogramma malware en informatie over de release van de tool vindt. Dit bevat ook informatie over beheerders en gevorderde gebruikers, waaronder informatie over ondersteunde schakelopties voor de opdrachtregel.

Opmerkingen
Met het Microsoft-ondersteunings levenscyclus beleid wordt de MSRT niet langer ondersteund in Windows Vista of op een ouder platform. Ga voor meer informatie naar Microsoft Support Lifecycle.

Als u problemen ondervindt met een update van MSRT binnen Windows Update, raadpleegt u problemen met het bijwerken van Windows 10 oplossen.