Privacy in Windows 10

– een peulenschilletje?

André Reinink

Zijn Privatezilla en Bloatbox dé oplossing? Of doen we het op zijn 'Nerds' en passen we het 'hosts-bestand' van onze pc aan? (ook voor Linux- en macOS-gebruikers)

Het onderwerp privacy krijgt een steeds prominentere plek in ons leven. Eindelijk. Maar we zijn er nog lang niet.
Een tijdje geleden kreeg ik een via de eindredacteur een reactie van een lezer dat ik privacy niet serieus had genomen in mijn artikel. Als er één blad is dat het waard is om te lezen én dat dit onderwerp regelmatig ter sprake brengt dan is het de SoftwareBus wel. Ook in de voorgaande SoftwareBus was er weer het nodige te lezen.

Het probleem met privacy is dat het enigszins ongrijpbaar is. Je kunt wel inschatten hoeveel berichten je in je e-mailbox hebt gekregen of hoeveel websites je bezocht hebt, maar je kunt niet aangeven hoe vaak je privacy geschonden is. En toch hebben we er elke dag mee te maken. En toch doen de meeste gebruikers er vrijwel niets aan.

Als gewone gebruiker hebben we een beperkte invloed om de privacy online te verbeteren. Natuurlijk, we kunnen een privacy-vriendelijke browser nemen, we kunnen extra extensies of add-ons installeren. We kunnen het gebruik van openbare netwerken vermijden. We kunnen vage websites omzeilen. We kunnen een VPN-verbinding gebruiken. Het zijn allemaal mogelijkheden om je privacy te verbeteren en je online-veiligheid te verhogen. Maar je moet er wel zelf de nodige moeite voor doen, je moet zelf uitzoeken hoe het zit. Je moet zelf je Windows OS na een update langslopen om te kijken of alle 'vinkjes' wel op de stand privacy staan. En op een gegeven moment denk je 'laat maar'. Toch zijn er een aantal mogelijkheden om het allemaal net een tandje beter te doen.

Privatezilla

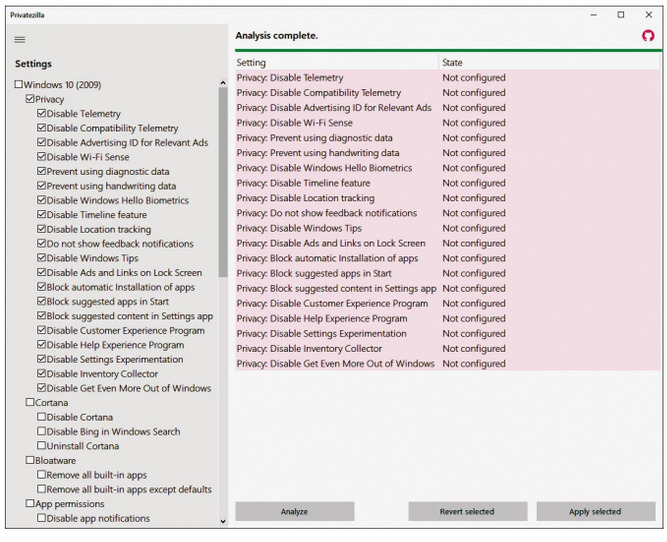
Euh, Privatezilla, FileZilla, Clonezilla, Mozilla?
Blijkbaar vinden auteurs van software het prettig om software te koppelen aan opensource termen als 'zilla'. Privatezilla klinkt als veel van hetzelfde, maar toch is Privatezilla interessant genoeg om nader te bekijken. Privatezilla is de opvolger van Spydish en is sinds de zomer van 2020 opensource.

Aan de slag

He programma kun je ophalen van de site van Builtbybel[1]. Een directe download vind je hier[2]. Het zip-bestand pak je uit naar een voor jou logische plek: een map ergens op een 'opslaglocatie'. Vroeger zou ik het begrip 'schijf' gebruikt hebben, maar schijven zijn steeds vaker een printplaat met geheugenchips, de inmiddels welbekende SSD.
Nadat je het programma uitgepakt hebt, kun je voor het gemak een snelkoppeling maken naar, bijvoorbeeld, je bureaublad. Start het programma op. Daarvoor zijn beheerdersrechten nodig.

Privatezilla interface

De interface is rechttoe-rechtaan. Links staan de items Privacy, Cortana, Bloatware, App permissions, Updates, Gaming, Windows Defender, Microsoft Edge en Security. Rechts verschijnen de instellingen. Bij aanvang is links *'Privacy'* aangevinkt en is het rechter gedeelte van het programmavenster leeg. Klik onder in het scherm op *'Analyze'*. De instellingen van *'Privacy'* en hun status komen nu in beeld.
Ik ga ervan uit dat je beseft dat klakkeloos items aanvinken en uitproberen niet handig is. Dus *'Remove all Built-in apps'* aanvinken en laten verwijderen lijkt me niet verstandig. Bezint dus eer ge begint.



Het scherm hierboven is een weergave van het openingsscherm. Ik heb het hoofdstuk 'Privacy' aangevinkt en vervolgens op 'Analyze' geklikt. Als voorbeeld ga ik alle onderdelen van 'Privacy' blokkeren. Ik klik op *'Apply selected'*, de status verandert van *'Not configured'* in *'Applied'*. Als ik daarna op *'Analyze'* klik, hebben alle onderdelen de status *'Configured'*. Ik kan dit ook weer terugzetten met *'Revert selected'*.

Je kunt een hoofdstuk in een keer configureren of per item. Elk item wordt, als je er met de muis boven beweegt, duidelijk(er) gemaakt door middel van een korte uitleg in het Engels. Probeer het zelf uit; dan wordt de werking je snel duidelijk.
Als je het hoofdstuk Privacy hebt gehad, kun je ook eens kijken naar de andere hoofdstukken. Ik weet zeker dat er opties zijn die voor jou van toepassing zijn.

Kan het ook anders?

Maar je kunt dit allemaal toch ook gewoon via de gebaande paden uitvoeren? Ja, dat klopt. Maar het grote voordeel is toch wel dat alle opties keurig gerangschikt staan. En na een update van het OS loop je met behulp van Privatezilla de instellingen even na en past ze zo nodig aan. Et voilà!
Een instructiefilmpje over Privatezilla kun je hier[3] vinden.

Bloatbox

In eerste instantie lijkt het een samentrekking van ‘bloot’ en ‘botox’. En misschien is dat nog niet zo gek geassocieerd. Bloatbox was ooit bedoeld om te integreren met Privatezilla. De auteur wilde enerzijds Privatezilla niet te groot maken, maar ‘mean and lean’ houden, en anderzijds wilde hij Bloatbox toch laten bestaan. Vandaar dat Bloatbox een stand-alone programma is geworden.

De standaardversie of de Community-version?

Bloatbox is een, wat mij betreft, geslaagde poging om een Windows 10 gebruiker op duidelijke wijze in een overzicht de apps te tonen die aan boord van jouw systeem zijn en desgewenst op een simpele en comfortabele manier te verwijderen. De standaardversie heeft ruim voldoende opties voor de standaardgebruiker. Wil je meer opties dan is er een *‘Community-version’* beschikbaar. Deze versie heeft als extra opties o.a.:

- herinstalleren van voorgeïnstalleerde apps
- verwijderen van specifieke voorgeïnstalleerde apps
- Startmenu tegels ‘unpinnen’
- deïnstalleren van OneDrive
- Windows Defender uitschakelen (niet verstandig)
- Blokkeren telemetrie via Firewall en hosts-bestand

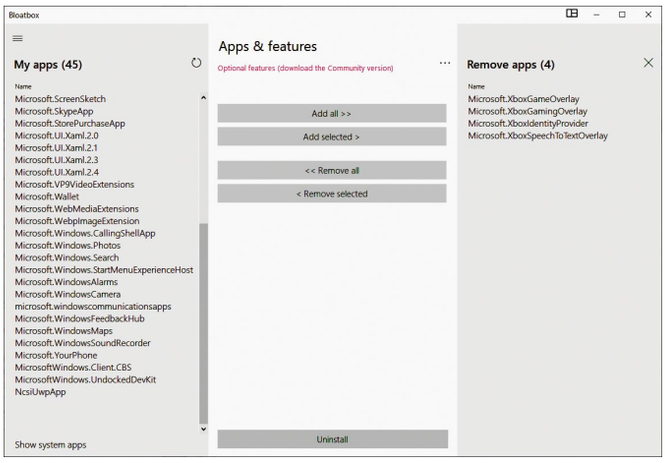
Ook hier geldt: bezint eer ge begint.

Aan de slag

Net als Privatezilla is ook de werking van Bloatbox intuïtief en simpel. Het programma downloaden, het zip-bestand uitpakken naar een een zelf te kiezen map. Eventueel een snelkoppeling maken. Start **‘Bloatbox.exe’**. Er wordt een index van alle apps in tekstformaat in dezelfde map vastgelegd. Aansluitend verschijnt het overzichtsscherm van Bloatbox. Links staan alle apps overzichtelijk gerangschikt. In het midden staan commando’s in de vorm van knoppen. Rechts is plaats ingeruimd voor alle apps die geselecteerd zijn om verwijderd te worden.
Enige tijd geleden gaf Microsoft aan dat bij de nieuwere versies van Windows 10 voorgeïnstalleerde apps gedeïnstalleerd konden worden. Helaas blijkt dat toch niet voor alle (ongewenste) apps van toepassing is. Misschien is dat wel in de actuele update gelukt. Bloatbox knapt het klusje wel goed voor je op. Ik krijg na opstart een lijst met 42 apps voorgeschoteld.

Ondertussen

Welke apps jij van jouw systeem wilt verwijderen is natuurlijk een persoonlijke keuze. Omdat ik geen spelletjesfanaat ben zou ik bijvoorbeeld apps waarvan de naam begint met *‘Microsoft.Xbox’* kunnen verwijderen.
Ik selecteer alle apps die beginnen met Microsoft.Xbox en klik daarna op *‘Add selected’*. De geselecteerde apps verschijnen in het rechter deel van het programmascherm. Als laatste klik ik op de knop *‘Uninstall’*, onder aan het middelste deel van het scherm. Aansluitend krijg ik de melding *‘Succesfully removed:’* gevolgd door de namen van de vier verwijderde ‘Xbox apps’.



De smaak te pakken

Evenzo zou ik apps als Microsoft People of Microsoft Wallet kunnen verwijderen. En misschien nog wel meer. Een gewaarschuwd mens telt nog steeds voor twee. Wees dus voorzichtig met het deïnstalleren van apps en zeker met het deïnstalleren van System-apps. Sommige System-apps kúnnen overigens niet gedeïnstalleerd worden omdat deze nodig zijn voor de ‘Windows 10-ervaring’ zoals de auteur het noemt. Denk daarbij bijvoorbeeld aan .NET Framework.

Resumerend

Het programma Bloatbox waarschuwt gebruikers duidelijk voor onverstandige acties. Klein minpuntje: het programma is Engelstalig. Ook voor dit programma geldt: probeer het eens uit en de werking wordt je al snel duidelijk.
Advies: als je een ‘enthousiaste’ pc-gebruiker bent, maak dan eerst een back-up van je systeem of zorg op z’n minst voor een herstelpunt.

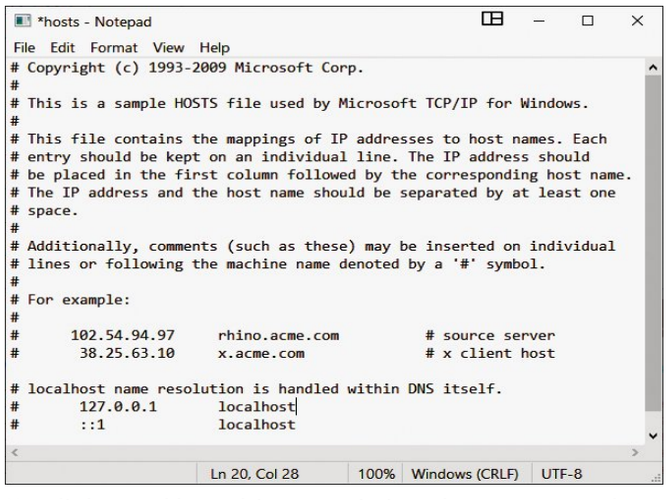
Het hosts-bestand aanpassen

Ik heb nooit begrepen waarom deze methode zo weinig bekend is en amper wordt toegepast. Eerst een korte introductie.

Als je achter je pc zit of een ander apparaat gebruikt met de mogelijkheid om webpagina’s op te vragen, gebeurt er het volgende. Je typt op de url-balk een webadres in, www.facebook.com, bijvoorbeeld. De data waarmee deze webpagina op jouw device wordt getoond komt van meerdere servers op verschillende locaties in de wereld. Jouw browser kijkt eerst of de te tonen data al lokaal (op jouw device) aanwezig is. Zo niet dan wordt de data opgehaald en aan de webpagina toegevoegd die je wilt openen. Ad-blockers werken ook op die manier: ze beoordelen de op te halen data voordat deze op je scherm getoond wordt.
Op computers vind je een zogenaamd hosts-bestand[4]. Met dit bestand kun je specifieke domeinen ‘blokkeren’. En dat heeft een paar grote voordelen: het werkt effectief en het is browseronafhankelijk.

Aan het werk

Een voorbeeld van een hosts-bestand:

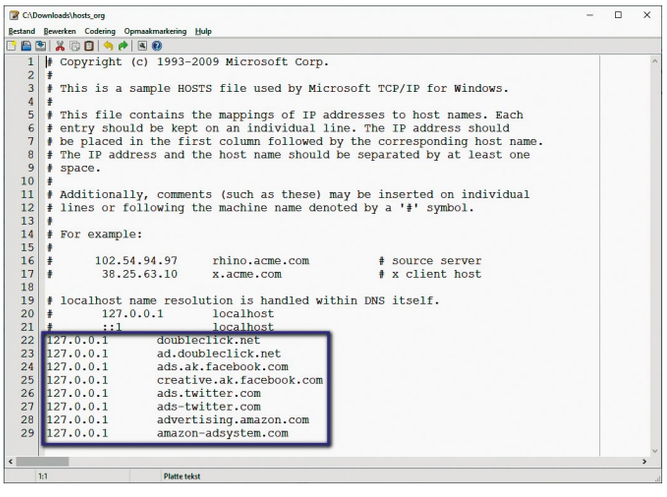


Met dit bestand bepaal je wat er in jouw browser getoond

gaat worden. Het bestand staat in het Windows-OS onder **c:\windows\system32\drivers\etc\hosts** en in Linux en bij macOS onder **/etc/hosts**.
Het bestand kan alleen met beheerdersrechten worden aangepast. In principe is de procedure van het aanpassen van het bestand van de genoemde besturingssystemen identiek: bestand openen als beheerder en de inhoud aanpassen.

Een stapje verder

Als voorbeeld ga ik acht domeinen blokkeren die wereldwijd de meeste advertenties aandragen:
doubleclick.net, **ad.doubleclick.net**, **ads.ak.facebook.com**, **creative.ak.facebook.com**, **ads.twitter.com**, **ads-twitter.com**, **advertising.amazon.com** en **amazon-adsystem.com**. Ik pas het hosts-bestand aan en dat ziet er dan zo uit:



De domeinen in het voorbeeld worden voorafgegaan door adres **127.0.0.1**, het interne adres van jouw computer. Als een van de domeinen opgevraagd wordt, zoekt het naar de data op **127.0.0.1** en vindt daar dus niets. De data wordt dus niet in je browser getoond. Als daar wel data gevonden wordt en je wilt dat niet, dan moet je de cache van je browser opschonen. Het interne adres **127.0.0.1** en de te blokkeren domeinnaam moeten gescheiden zijn en ze mogen niet aan elkaar geschreven worden.

Dat kan beter en efficiënter

Zelf het bestand regel voor regel aanpassen is voor een paar domeinen nog wel te doen, maar wat als er een organisatie is die het 'vuile werk' al voor je opgeknapt heeft? Dat is '**MVPS**'[5,6]. Het hosts-bestand dat we gaan gebruiken is hier[7] te downloaden. Pak het bestand uit op een plek naar keuze. '*Hosts.zip*' bevat vijf bestanden: drie tekstbestanden, een batchbestand en een door MVPS aangemaakt hosts-bestand. Het batchbestand is specifiek bedoeld voor Windows-gebruikers. Met dit batch-bestand kun je het hosts-bestand op jouw pc door het MVPS aangeleverde hosts-bestand laten vervangen. Voer het batch-bestand uit (rechter muistoets, uitvoeren als beheerder). Het is de moeite waard om het bestand '*readme.txt*' te lezen. Hierin staan belangrijke tips en aanvullende informatie. Helaas alleen in het Engels, maar alles wordt wel heel duidelijk beschreven. Verplichte leeskost lijkt me.

Linux en Mac

Een methode die voor Linux- en Mac-gebruikers gebruikt kan worden is de handmatige methode. Je kunt net als in mijn eerste voorbeeld, met de acht advertentiedomeinen, de te blokkeren domeinen in het hosts-bestand zetten. Handiger is om het MVPS bestand 'HOSTS' uit het zipbestand handmatig naar de juiste locatie op jouw systeem te plaatsen en het oude bestand te overschrijven. Maak zelf een kopie van het originele bestand. Op dit moment staan er een kleine 11.000 te blokkeren domeinen in het hosts-bestand van MVPS. Maar voel je vrij zelf een keuze te maken voor de te blokkeren domeinen.

0.0.0.0 *of* 127.0.01?

In mijn eerste voorbeeld zie je dat ik **127.0.0.1** als intern adres gebruikt heb. En ik ben daar niet de enige in. Als je echter het bestand van MVPS gebruikt zal het je misschien opvallen dat zij adres **0.0.0.0** gebruiken. Adres **127.0.0.1** wordt ook wel het loopback-adres genoemd of 'local host'. **0.0.0.0** is een niet-routeerbaar adres dat aangeeft dat het een ongeldig adres is. Op diverse forums is er discussie over wat in het geval van het hosts-bestand de beste of juiste keuze is. Volgens experts is het gebruik van adres **0.0.0.0** sneller, efficiënter. Vaak wordt daarbij wel opgemerkt dat de snelheidsresultaten browserafhankelijk zijn. In mijn testomgeving heb ik geen snelheidsverschillen opgemerkt.

Tot slot

In de SoftwareBus wordt het onderwerp privacy regelmatig besproken. Meestal in de vorm van gedegen informatie. Soms aangevuld in de vorm van duidelijk onderbouwde tips en trucs. Dat ook niet-professionele auteurs een waardevolle bijdrage kunnen leveren is duidelijk.
Helaas is privacy vaak een saai onderwerp. Liever horen we sappig nieuws over overheden die al dan niet illegaal spioneren. Of spannende berichten over overheden die apparatuur van Huawei verbieden omdat men denkt dat dergelijke apparatuur een 'backdoor' heeft. Daarbij is men schijnheilig bezig, vind ik. Want laten we wel wezen: Apple en Google zullen dat ook hebben. En heel veel Nederlandse klanten van KPN hadden vroeger een modem van Siemens en tegenwoordig een modem van ZTE (Experiabox). Een bedrijf met militaire affiniteit, net als Huawei. En over apps als TikTok zullen we het verder maar niet hebben. Apropos: de app van Albert Heijn is ook een discussie waard.

Gemak dient de mens, of …

Helaas geldt voor veel mensen dat het gemak van apparatuur en bijbehorende software de aandacht voor privacy naar de achtergrond drukt. Op een gegeven moment berusten mensen erin en laten alles zoals het is. Of men zegt: *'Ik heb toch niets te verbergen'*.
Een plan de campagne zou kunnen zijn:
- (nog) meer informatie aanbieden aan gebruikers
- kritisch zijn in het gebruik van apparatuur en software
- zo mogelijk druk zetten op lokale, landelijke of Europese overheden. Gelukkig is Europa kritisch op het gebied van privacy. Of dat genoeg is moet nog blijken. Het zou mooi zijn dat binnen Europa de neuzen dezelfde kant op staan. Waarom wordt voor overheidsgebruik in het ene EU-land Microsoft 365 en Whatsapp niet toegestaan en mag dit in het andere EU-land wel?

HCC?

Ooit was de HCC de grootste vereniging van computergebruikers met meer dan 223.000 leden. Wat zou het mooi zijn als de HCC de handen ineensloeg met andere computergebruikersverenigingen in Europa, om dit samen aan de orde te stellen.

Voor nu

Blijf nuchter in het gebruik van je computer en bijbehorende apparatuur. En onderschat daarbij ook niet de mogelijkheden van de smartphone. Beetje bij beetje neemt deze de plaats van de pc volledig over.

Links:

1) Builtybel:
   https://www.builtbybel.com/ https://bit.ly/3pY2LTQ
2) Privatezilla Opensource:
   https://www.builtbybel.com/blog/12-company-announcements/39-spydish-becomes-privatezilla-open-source
   https://bit.ly/2KjKeAO
3) Instructiefilmpje Privatezilla:
   https://github.com/builtbybel/privatezilla/blob/master/assets/intro.gif https://bit.ly/2ITjBCi
4) Meer informatie over het hosts-bestand
   https://www.schoonepc.nl/nieuwsbrief/hosts-bestand_aanpassen.html https://bit.ly/2UIW7T1
5) MPVS:
   https://winhelp2002.mvps https://bit.ly/2UNTTSa
6) Hosts-bestand:
   https://winhelp2002.mvps.org/hosts.htm
   https://bit.ly/39240vd
7) https://winhelp2002.mvps.org/hosts.zip