computertotaal.nl

Microsoft's spionage-software uitschakelen in Windows 10

Door: Edmond Varwijk

| 11 april, 14:19

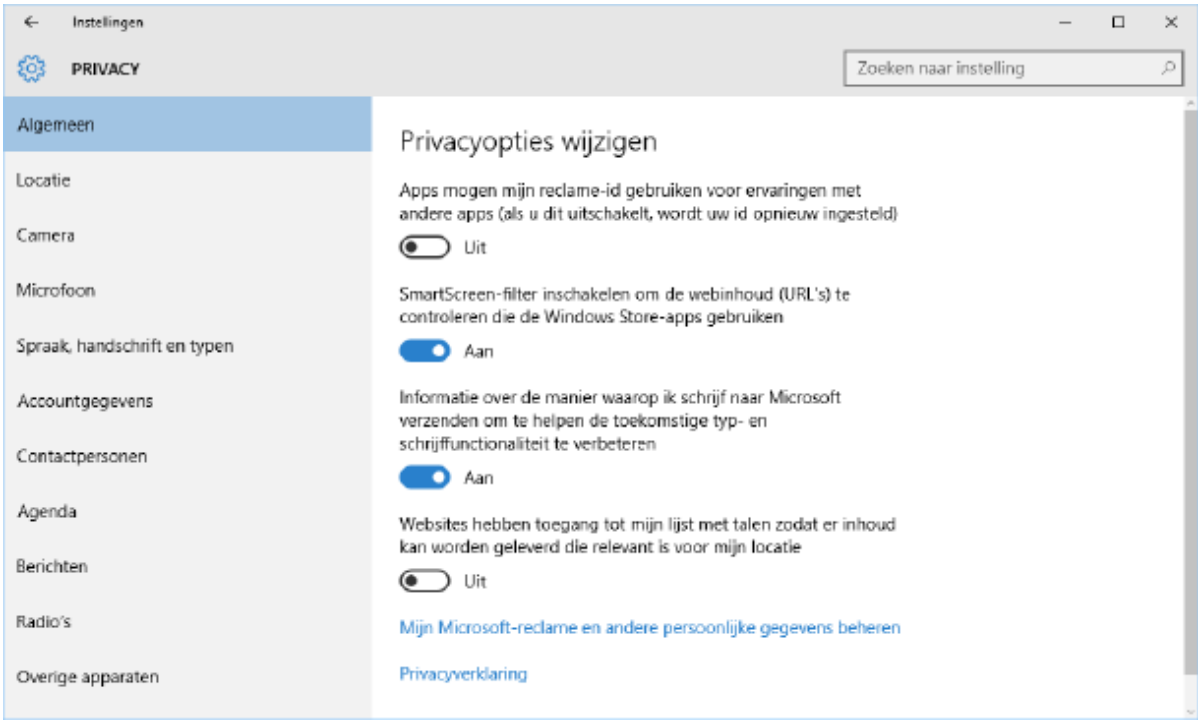
How To

Wanneer iets gratis wordt weggegeven, ben jij het product. Dat werd pijnlijk duidelijk met de upgrade naar Windows 10. Het besturingssysteem verzamelt en deelt informatie over jouw gebruik met in elk geval Microsoft. Veel van de functies kun je uitschakelen, maar lang niet alles. Dat pakken we aan.

Windows 10 is de eerste versie van het besturingssysteem met ingebouwde spyware. Het controleert en logt bijvoorbeeld continu je locatie en al jouw activiteiten en deelt deze gegevens met zichzelf en derden. Er is veel kritiek op deze handelswijze, maar Microsoft lijkt er doof voor. In een blogpost licht het bedrijf slechts toe dat het die gegevens verzamelt om "het product Windows beter voor jou te laten werken" en dat je "als gebruiker zelf bepaalt welke informatie wordt verzameld". Lees ook: Zo claim je je recht op privacy terug.

Maar de realiteit is anders: slechts een deel van de gegevensverzameling kun je uitschakelen, een ander deel niet of alleen tegen een te hoge prijs. Zo is de SmartScreen-techniek die websites scant op phishing- en malware een prima zaak, maar waarom moet de informatie over elke site die je bezoekt, ook

meteen gedeeld worden met Microsoft zelf? Tevens heeft elke Windows 10-pc een uniek reclame-ID dat gebruikt wordt om de pc anoniem te identificeren, maar wat als je helemaal die reclames niet wilt, ook niet anoniem?



De privacyopties in Windows 10 waarmee je een deel van de spyware kunt uitschakelen.

Hoe gek Microsoft denkt dat we zijn?

Een belangrijke rol in de Microsoft-spyware is weggelegd voor een service genaamd DiagTrack. Een service is een onderdeel van Windows die ongemerkt op de achtergrond zijn werk doet. Er zijn talloze services, vaak nuttig, maar deze DiagTrack is de service die op de achtergrond privégegevens, de browse- en zoekgeschiedenis en informatie over de pc verzamelt en deelt met Microsoft. Veel gebruikers spoorden de service daarom op en schakelden die uit. Toen Microsoft in november een grote update voor Windows 10 uitbracht, bleek die service ineens verdwenen, ook op de pc's van mensen die de service niet zelf uitgeschakeld hadden.

Had Microsoft geleerd? Integendeel, helaas. Microsoft bleek de spionageservice met de update namelijk slechts een andere naam gegeven te hebben én op alle pc's weer ingeschakeld. Oók pc's waar de dienst wél was uitgeschakeld. En dat zonder de gebruiker hierover te informeren. Een pijnlijk praktijkvoorbeeld van hoe het bedrijf tegenwoordig omgaat met (privacy)klachten van gebruikers: negeren, in de doofpot stoppen en waar nodig verbergen. Terwijl Microsoft juist zei voornemens te zijn extra veel te luisteren naar feedback van gebruikers bij de ontwikkeling van Windows 10.

DiagTrack uitschakelen

Voor wie het wil controleren: DiagTrack (oftewel Diagnostic Tracking Service) heet nu 'Connected User Experiences and Telemetry'. Een mooiere naam voor dezelfde drol. Wil je deze service alsnog of opnieuw uitschakelen? Druk op het toetsenbord de toetscombinatie **Windows-toets+R** in. Voer in het uitvoeren-vak het commando services.msc in gevolgd door **Enter**. Zoek in de lijst met services naar Connected User Experiences and Telemetry. Dubbelklik erop en kies Stoppen. Zet het Opstarttype daarna op Uitgeschakeld.

Wapen jezelf

Kortom. Microsoft lijkt niet het beste met z'n gebruikers voor te hebben. Kun je er dan niets tegen doen? Jazeker wel. Je kunt op zoek gaan naar de verschillende opties voor de privacygevoelige functies en die uitschakelen. Dat is niet moeilijk, maar Microsoft heeft er vermoedelijk bewust voor gekozen alle voor privacy belangrijke opties te verspreiden over een groot aantal onderdelen binnen de instellingen. Je moet dus op zoek en er is flinke kans dat je er een of enkele mist wanneer je niet trouw een lijstje afwerkt.

Een deel van die dataverzameling is in de instellingen van Windows 10 uit te schakelen. Een volledige beschrijving van hoe dit moet en hoe je een aantal belangrijke privacyschenders in de Windows-instellingen de kop omdraait, vind je op onze website.

Tools die helpen

Er is een flink aantal programma's verschenen die helpen de privacyopties in Windows 10 te beheren. Wees kritisch welke je download en installeert. Installeer zeker privacytools alleen van vertrouwde websites en controleer elke download via VirusTotal.com (zie kader Malware-alarm?) op malware voordat je het programma installeert. Gebruik de installatieopties om ongewenste extra software weg te laten.

Malware-alarm?

We noemen in dit artikel een drietal tools die je kunnen helpen met tegengaan van spionage door Windows. Deze hebben we natuurlijk alle drie door VirusTotal.com laten beoordelen. VirusTotal is een dienst (tegenwoordig van Google) die sites en software kan scannen op de aanwezigheid van virussen en malware en daar de producten van tientallen verschillende beveiligingsbedrijven voor gebruikt. VirusTotal rapporteert dat Destroy Windows 10 Spying helemaal schoon is. Van DoNotSpy10 zijn twee versies: de donatieversie van 5 dollar is schoon, maar de gratis versie wordt terecht melding gemaakt van de aanwezigheid van adware. Tijdens de installatie kun je overigens voorkomen dat deze OpenCandy-reclamesoftware op je systeem komt te staan. Bij W10Privacy geven twee van de ruim vijftig scanners van VirusTotal een melding, maar we gaan ervan uit dat dat een vals positief is.

Maar het kan dus gebeuren dat je beveiligingssoftware bij het downloaden van deze programma's alarm slaat, zelfs als VirusTotal de software als veilig classificeert. Dat heeft ermee te maken dat de heuristische scanner van sommige beveiligingssoftware het installatiebestand onterecht aanmerken als onveilig.

Lees verder >>

computertotaal.nl

Microsoft's spionage-software uitschakelen in Windows 10

Door: Edmond Varwijk

| 11 april, 14:19

How To

Wanneer iets gratis wordt weggegeven, ben jij het product. Dat werd pijnlijk duidelijk met de upgrade naar Windows 10. Het besturingssysteem verzamelt en deelt informatie over jouw gebruik met in elk geval Microsoft. Veel van de functies kun je uitschakelen, maar lang niet alles. Dat pakken we aan.

Destroy Windows 10 Spying

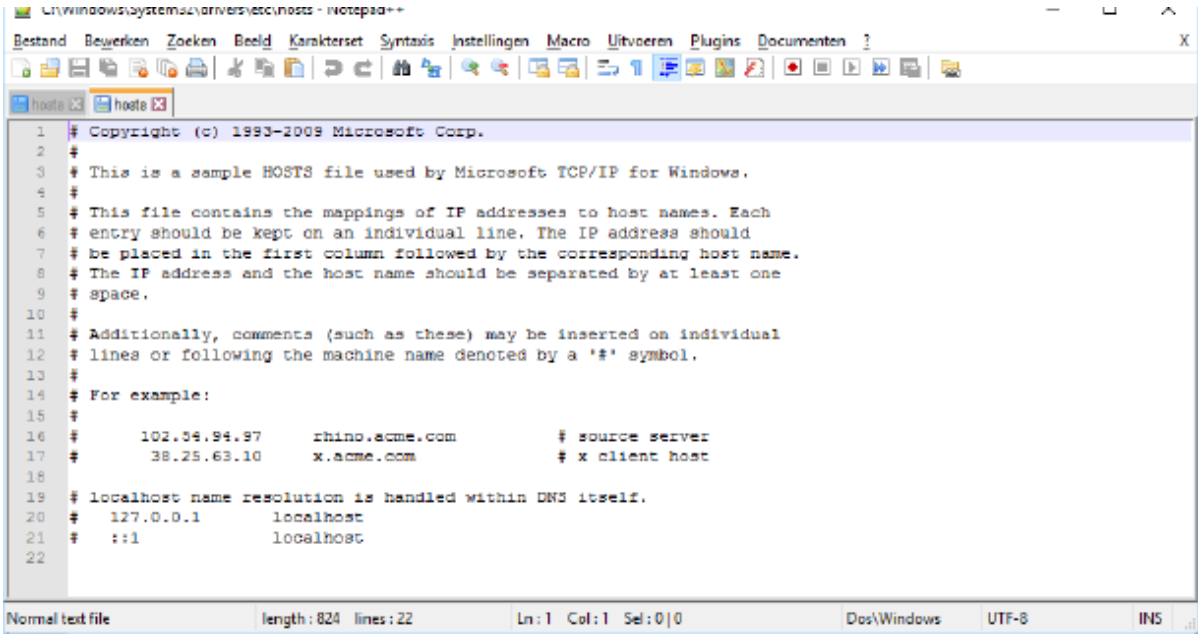
De titel van deze tool is even vanzelfsprekend als de werking en dat is goed. Want je wilt gewoon het spioneren stoppen en deze regelmatig bijgewerkte tool doet dat. Download Destroy Windows 10 Spying (DWS) via de groene knop met Latest release op http://dws.wzor.net (scrol daarvoor iets naar onder). Op de site staat ook een link naar de broncode (source code) die op Github is gepubliceerd. DWS is namelijk opensource, wat zeker bij een tool als dit een geruststelling is. Daarbij is het een portabele app, geen installatie-ellende dus, het bestand DWS_Lite.exe opstarten is voldoende. DWS verwijdert alle spyware die door Microsoft is ingebouwd in Windows 10 (en ook in Windows 7, 8 en 8.1). Sommige delen worden echt verwijderd, daar waar dat niet kan worden ze uitgeschakeld.

Destroy Windows 10 Spying is opensource, wat een gerust gevoel geeft.

Phone home-firewall

Een belangrijke rol in DWS is weggelegd voor het hosts-bestand en de Windows Firewall. Hoewel heel verschillend kun je met beide onderdelen uitgaande verbindingen aanpassen. Met de firewall kun je ze gericht stoppen, met het hosts-bestand kun je ze omleiden. Het hosts-bestand bevat een reeks namen van servers en websites en bijpassende IP-adressen. Door hier sites aan toe te voegen of verwijzingen te veranderen kun je niet alleen onbetrouwbare websites blokkeren, maar ook de communicatie met de eigen servers van Microsoft.

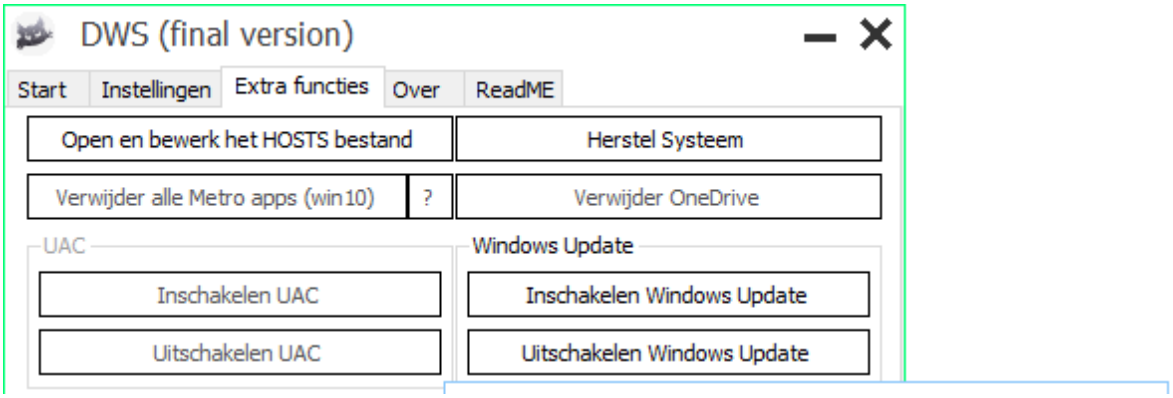
DWS past zowel de Windows Firewall als de verwijzingen in het hosts-bestand zo aan dat IP-adressen van Microsoft-servers, waar de logs van jouw computergebruik naartoe worden gestuurd, geblokkeerd worden. Voor wie vooraf een kopie wil veiligstellen: het hosts-bestand is in Windows te vinden via C:\Windows\System32\Drivers\etc\hosts.

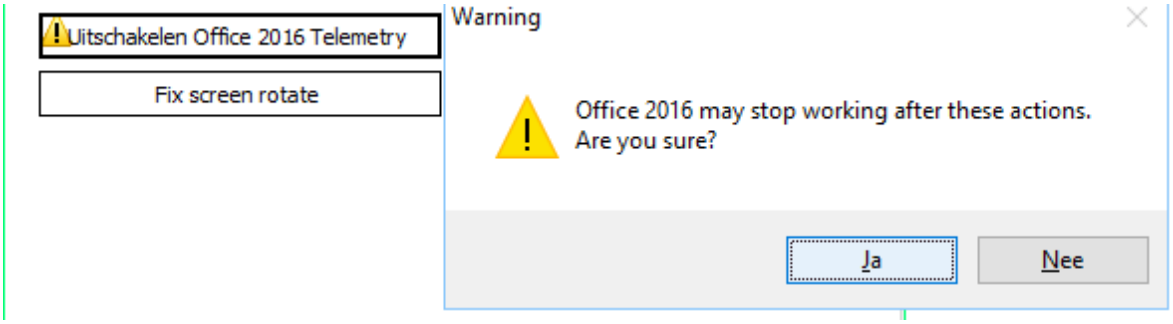


Het hosts-bestand is al sinds de Windows NT-jaren een veelgebruikt middel om de communicatie door Windows te beïnvloeden.

Office 2016 Spyware

Niet alleen Windows, maar ook Office houdt bij wat je allemaal doet met de pc. Zo worden de namen van de documenten die je opent, de add-ins die je gebruikt en ook systeem- en gebruikersinfo weer met Microsoft gedeeld. Ook metadata van documenten wordt bekeken, maar niet de inhoud. Destroy Windows 10 Spying biedt bij de Extra functies ook een optie Uitschakelen Office 2016 Telemetry waarmee je deze kunt uitschakelen. De functie is echter nog erg experimenteel en Office is erg gevoelig. DWS waarschuwt zelf al dat het uitschakelen van deze Office-spyware kan leiden tot het niet meer correct werken van Office en we kunnen dat helaas bevestigen.





De dataverzameling van Office laat je beter ongemoeid.

Apps afsluiten

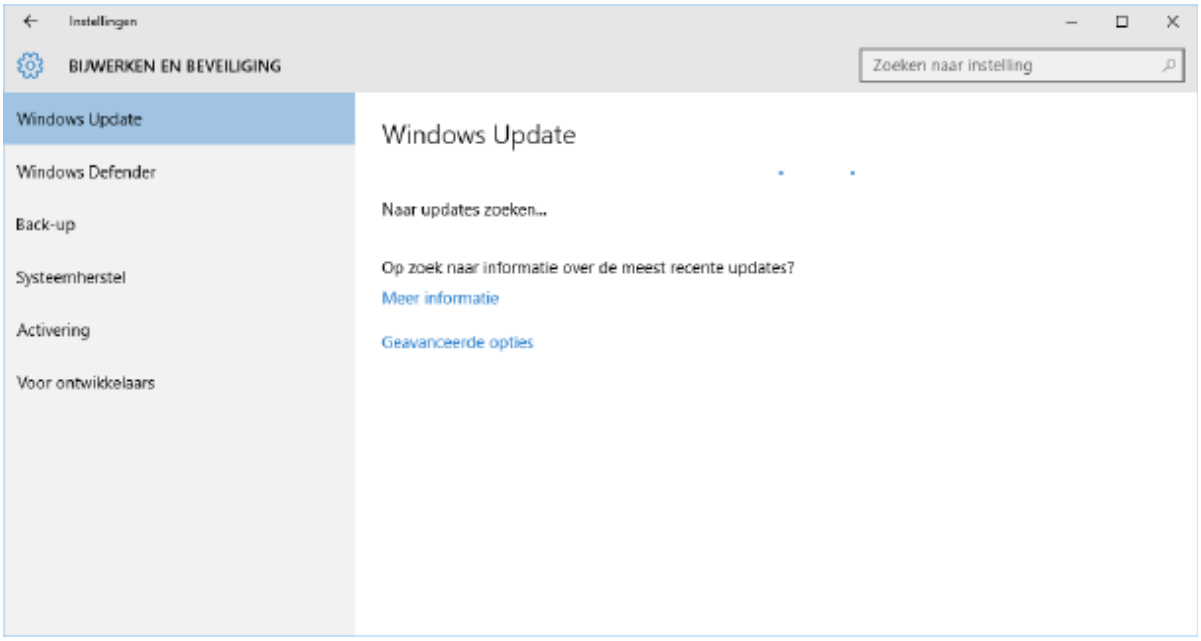
De functies van DWS vind je op het tabblad Instellingen. De bovenste zeven functies in de versie die wij getest hebben, hebben allemaal impact op de privacyinstellingen en richten zich dus nadrukkelijk op de spionage door Microsoft. De onderste functies doen dat niet, deze richten zich op de Metro-apps. Opnieuw stop je de spionage en vooral het loggen van het gebruik door deze apps. Wil je ook deze apps verwijderen, zet dan een vinkje bij Verwijder Windows 10 Metro Apps. Pas dan worden de onderste functies actief en kun je in dit geval ook apps uitsluiten.

Ga dan naar het tabblad Start en klik op Destroy Windows 10 Spying om Windows zo aan te passen dat de spionage wordt gestopt. DWS laat vervolgens heel duidelijk zien wat er allemaal wordt aangepast, welke wijzigingen in de firewall, aanpassingen in het hosts-bestand, het is allemaal regel voor regel te volgen. Aan het einde laat hij zien welke acties zijn gelukt.

Windows Update

Windows 10 is volgens Microsoft niet langer een product, maar een service. Het verschil is dat een service altijd geüpdatet wordt, een product niet. Een product koop je en gaat dan lange tijd ongewijzigd mee, een service kan elk moment worden aangepast. Deze verandering is goed te merken aan Windows Update. In

plaats van een patchdag elke maand, komen er nu continu updates uit. En ook het verschil vervaagt tussen een update om problemen op te lossen en een update die functies toevoegt. Een update kan ook nieuwe privacygevoelige functies toevoegen aan Windows of een instelling aanpassen. Dat geldt zeker ook voor de grote updates die Microsoft nu ongeveer elk half jaar wil uitbrengen, zoals de november-update waarmee echt nieuwe functies aan Windows werden toegevoegd, maar waarmee ook de DiagTrack-spywareservice werd hernoemd en ingeschakeld.



Windows Update is niet meer de onverdachte systeemverbeteraar die het lange tijd is geweest.

Lees verder >>

computertotaal.nl

Microsoft's spionage-software uitschakelen in Windows 10

Door: Edmond Varwijk

| 11 april, 14:19

How To

Wanneer iets gratis wordt weggegeven, ben jij het product. Dat werd pijnlijk duidelijk met de upgrade naar Windows 10. Het besturingssysteem verzamelt en deelt informatie over jouw gebruik met in elk geval Microsoft. Veel van de functies kun je uitschakelen, maar lang niet alles. Dat pakken we aan.

Risico

Wil je er zeker van zijn dat je geen nieuwe spyware van Microsoft ontvangt of dat men met een update, spionagefuncties die uitgeschakeld waren weer activeert dan kun je natuurlijk zelf Windows Update uitschakelen en ook DWS kan dat doen. Op het tabblad Extra functies vind je ook een knop om met één klik Windows Update uit te schakelen. Dit is echter wel een functie om goed over na te denken en eerlijk gezegd raden we dit af. Schakel je Windows Update uit, dan betekent dat je bewust het risico neemt dat bekende kwetsbaarheden in Windows (inclusief degene die al misbruikt worden door malware of hackers) op jouw pc niet opgelost worden. Het gevolg daarvan kan zijn dat je in je streven Microsoft buiten de deur te houden juist andere partijen met veel meer vriendelijke bedoelingen toelaat. Een te groot risico.

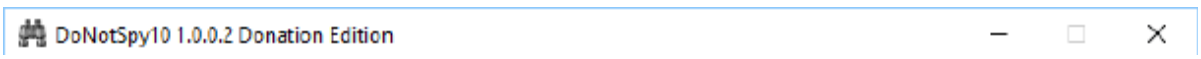
Als alternatief kun je regelmatig DWS nog eens starten en zijn werk opnieuw laten doen. Doordat DWS bij het opstarten controleert of er van het programma zelf niet een nieuwere versie beschikbaar is en die dan snel download, profiteer je dan bovendien ook nog van mogelijke nieuwe of verbeterde antispionagefuncties die zijn toegevoegd.

DoNotSpy10

Een handige alternatieve tool en duidelijk minder ingrijpend dan Destroy Windows 10 Spying is DoNotSpy10. Wil je het programma gratis gebruiken, vink dan tijdens de installatie de OpenCandy-reclamesoftware uit. Voor een paar euro koop je een OpenCandy-vrije versie. Je downloadt deze advertentievrije editie van DoNotSpy10 hier.

Nieuw in vergelijking met een eerdere versie is de kleurcodering die de verschillende opties meekrijgen. Opties die zonder meer veilig uitgeschakeld kunnen worden zijn groen, de opties met iets meer risico of opties die ook echt de functionaliteit van Windows 10 raken, zijn oranje of rood. Zeker de rode zijn alleen met grotere terughoudendheid te gebruiken, al is het wel handig dat je ook die vanuit dit ene overzicht kunt instellen. Het uitschakelen van bijvoorbeeld de Windows Store Updates (oranje) en Windows Update (rood) is af te raden omdat je daarmee ook voorkomt dat beveiligingsfouten in Windows niet of pas later worden opgelost.

Bij elke functie komt een korte toelichting, soms is even googelen voor meer informatie aan te bevelen. Wil je een functie uitschakelen, plaats dan een vinkje ervoor en klik op Apply. Gebruik geen Check All, omdat dan ook alle rode opties worden gekozen.



Terughoudendheid is vereist bij de oranje en rood gemarkeerde opties in DoNotSpy10.

W10Privacy

Duitsers zijn gemiddeld genomen kritischer dan andere Europeanen als het gaat om privacy en dat is mogelijk de reden dat ook de tool W10Privacy uit dat land komt. W10Privacy doet in essentie hetzelfde als DoNotSpy10, maar uitgebreider. Wat DoNotSpy10 op één overzicht op hoofditem bij elkaar houdt, is door de makers van W10Privacy helemaal uit elkaar getrokken over 14 tabbladen, elk bomvol opties. Gelukkig zijn de opties net zoals bij DoNotSpy10 voorzien van kleurcodering (groen, oranje, rood) die de impact aangeeft.

Voor een toelichting op een bepaalde functie, zet je de muis erboven. Desondanks zijn tabbladen als Telemetry en Firewall lastig te gebruiken. Hier kun je van services en applicaties waarvan bekend is dat ze informatie verzamelen of delen het uitgaande verkeer blokkeren. Maar om sommige instellingen te wijzigen, is het nodig W10Privacy met administratorrechten te starten. Na elke wijziging start het programma zichzelf opnieuw op om de gewijzigde instellingen correct weer te geven. Niet alle instellingen worden overigens ook echt succesvol toegepast. W10Privacy is veelbelovend, maar duidelijk minder klaar voor gebruik dan de andere tools.

Tenslotte

Windows 10 is fantastisch en vernieuwend. Dat maakt het juist zo jammer dat Microsoft ervoor gekozen heeft met het nieuwe besturingssysteem zo schaamteloos de Windows-gebruikers te besnuffelen. Gelukkig kun je uiteindelijk jezelf ook wapenen tegen de nieuwsgierigheid van de Amerikaanse softwarereus en voorkomen dat informatie over jou die jij niet wilt prijsgeven bij Microsoft bekend wordt. Met de stappen en de tools in dit artikel doe je immers ook niets anders dan wat Microsoft meteen al zelf had moeten doen en minimaal in de instellingen had moeten aanbieden.