Privacy en veiligheid in Windows

Ton Valkenburgh

Naar aanleiding van een webinar over dit onderwerp werd mij gevraagd er een artikel aan te wijden. Het is een wat uitgebreider verhaal geworden dan de webinar over hoe je de privacy en veiligheid bij het gebruik van Windows kunt verbeteren.

Inleiding

Het verdienmodel van veel organisaties verplaatst zich meer en meer naar het verzamelen van gegevens van ons, consumenten. Men wil hiermee zover komen dat, voordat je bedacht hebt wat je wilt aanschaffen, de advertenties je al worden voorgeschoteld. Daartoe is het nodig om gegevens van ons zoekgedrag, en nog meer van ons algemene gedrag, te verzamelen en te analyseren.

Als we zelf de touwtjes nog in eigen handen willen houden en geen marionetten willen worden, moeten we dus maatregelen nemen. Daarbij is belangrijk hoe we in ons dagelijks leven pc's, laptops, tablets, smartphones, het Internet of Things, en internet gebruiken. In dit artikel kijken we alleen naar wat we met onze Windows-pc of -laptop doen. Bedenk echter dat ook ons gedrag met die andere apparaten belangrijk is.

Privacy krijgt tegenwoordig veel aandacht in de pers en op de televisie. Het blijkt uit onderzoek dat we privacy en veiligheid belangrijk vinden. Helaas is ons gedrag hiermee niet in overeenstemming. Het lijkt er op dat andere overwegingen ons feitelijke gedrag bepalen. In dit artikel wil ik laten zien dat bij het gebruik van Windows de privacy en veiligheid kan worden verbeterd zonder dat het gebruiksgemak er onder te lijden heeft.
Er zijn veel wegen die naar Rome leiden. In dit artikel zie je de weg die ik heb gekozen, maar weet dat dit niet de enige weg is. Op internet is veel te vinden over hoe je je privacy en veiligheid kunt verbeteren.

Windows en de apps

Microsoft heeft bij zijn concurrenten ontdekt dat niet alleen met het verkopen van eigen software inkomsten te genereren zijn. Het businessmodel is daarom duidelijk aangepast. Microsoft ziet de advertentiemarkt en een app-store ook als bronnen van inkomsten. We kunnen dus verwachten dat het verzamelen van onze gegevens ook voor Microsoft steeds belangrijker wordt. Vandaar dat bij Windows 11 Home nu een Microsoft-account verplicht is bij het installeren. Hoewel dat in de pro-versie nog niet is vereist, zijn er al bedrijven die bij de introductie van versie 10 hebben besloten Windows niet meer te gebruiken.

Als consument kunnen wij natuurlijk besluiten om over te stappen op de pro-versie van Windows 11. Echter, het lijkt mij verstandiger om voorlopig Windows 10 te blijven gebruiken. Die versie wordt tenslotte tot diep in 2025 ondersteund. Mocht je echt Windows 11 willen gebruiken, dan kun je nog steeds Microsoft-account omzeilen (link 1.). Dat deze methode werkt is waarschijnlijk, omdat ook offline werken met Windows 11 mogelijk moet zijn.

Laten we beginnen bij de basis. Windows, en veel programma's die je geïnstalleerd hebt, verzamelen gegevens. Vaak is onduidelijk welke gegevens er verzameld worden. Bij veel programma's kun je het verzamelen uitzetten, maar is dan werkelijk alles uitgezet? Ook bij gratis programma's is het maar de vraag wat hun business-model is.

Bij het installeren van Windows wordt je een aantal vragen gesteld. Mijn advies is om hier altijd nee te kiezen. Mocht je dat niet hebben gedaan, dan helpt Spybot anti-beacon (link 2.) je er toch van af. Dit programma geeft je de optie om telemetrie van Windows en veel bekende programma's te blokkeren. Er zijn een gratis en een betaalde versie.

Afbeelding 1: Instellingen van Spybot Anti-Beacon

Onderzoek dus zelf of dat wat de betaalde versie extra blokkeert, voor jou relevant en van belang is. Het programma loopt alle instellingen bij het opstarten van Windows langs en zorgt er dus voor dat eventuele veranderingen door een update van Windows weer worden gecorrigeerd.

De internetverbinding

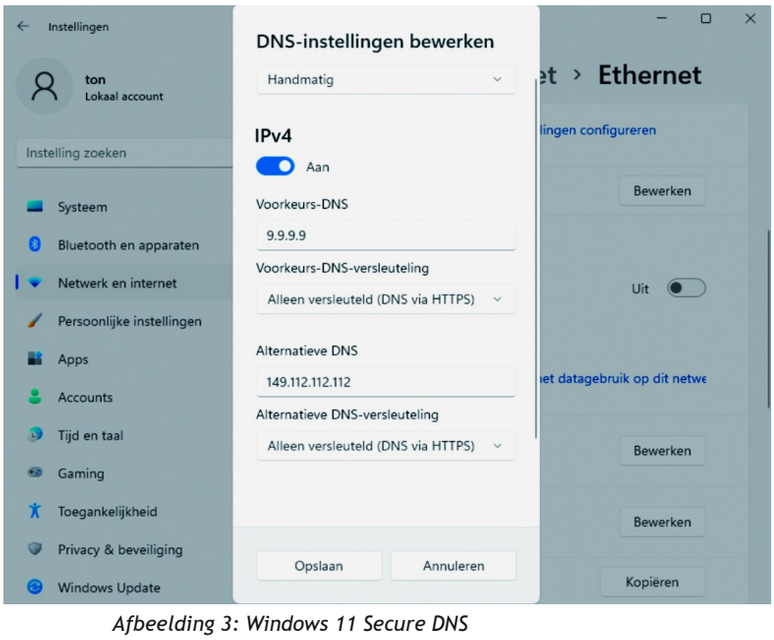
Zonder internet leven is niet makkelijk. Voor steeds meer services heb je internet nodig. Ook de overheid wil ons steeds minder fysieke post sturen en gaat er vanuit dat je internettoegang hebt.

Internet is echter opgezet in een tijd dat de focus niet op privacy en veiligheid lag. Op sommige punten loopt het daarom wat achter. Daarbij geldt dat ook jouw internetserviceleverancier niet altijd de laatste technologie installeert in zijn netwerk. Zo is bij de meeste leveranciers een verbindingsopbouw niet versleuteld. Daar kun je wat aan doen met *Secure DNS* (link 3.). Windows 10 ondersteunt het niet, maar door het programma *Simple DnsCrypt* (link 4.) is dit makkelijk te verhelpen. Het biedt trouwens meer functies, zoals o.a. een logboek.

De veilige DNS-server die ik altijd gebruik is de in Zwitserland gevestigde stichting *quad9*. Deze DNS-service biedt ook bescherming door filtering tegen malware, phishing, spyware en botnets. Je selecteert de gewenste DNS-server op het tabblad *Vertalers*. Voor het instellen van *Simple DnsCrypt* (afbeelding 2) verwijs ik naar mijn artikel in SoftwareBus 2021-4 (link 5.).

Afbeelding 2: Hoofdmenu van Simple DnsCrypt

Windows 11 ondersteunt *Secure DNS*. Ga in de netwerkconfiguratie naar *Netwerk en internet* > *Ethernet* > *DNS-server toewijzing* > *Bewerken* > *Handmatig*. Schakel hier *IP-4* in. Vul voor *Voorkeurs DNS* in: 9.9.9.9 en in het *pull-down menu* kies je *Alleen versleuteld (DNS via HTTPS)*. Bij *Alternatieve DNS-versleuteling* vul je 149.112.112.112 in en in het *pull-down menu* kies je *Alleen versleuteld (DNS via HTTPS)*. Je hebt nu beide adressen van Quad9 ingevuld (afbeelding 3).



Afbeelding 3: Windows 11 Secure DNS

Nu Microsoft steeds meer onze gegevens verzamelt, kun je hun firewall en virusscanner dan wel echt vertrouwen? Mijn ervaring is dat de virusscanner soms iets probeert te verhinderen waarmee ik telemetrie van Windows heb geblokkeerd. Ook zal Microsoft de eigen gegevensverzamelaars niet tegenhouden.

Ik gebruik dus een andere virusscanner en een andere firewall. Op internet zie je dat de verschillen op veiligheid niet groot zijn (link 6.). De ranking-lijstjes kunnen volgende maand trouwens weer anders zijn. Ik selecteer daarom op gebruiksgemak; dat verandert niet zo snel. Bij de selectie van een firewall raad ik aan er een te kiezen die ook checkt of programma's toegang tot internet mogen hebben. Zonealarm en F-secure doen dat.
Bij Zonealarm moet je zelf bepalen welke programma's je toegang tot internet geeft. Zonealarm heeft een gratis versie (link 7.) en een betaalde versie. F-secure (link 8.) bepaalt zelf welke programma's niet naar internet mogen. F-secure is niet gratis. Sommige internetleveranciers hebben echter een gratis licentie in hun pakket.

De browser

Veel van wat we op internet doen gaat via een browser. Welke browser is nu de beste keuze voor privacy en veiligheid? Ik gebruik Firefox. Dit is een browser die standaard al goede prestaties op het gebied van privacy en veiligheid levert. Hij staat niet bovenaan de ranglijst, maar biedt door zijn add-ons de mogelijkheid hem aanzienlijk beter te laten scoren. In SoftwareBus 2019-3 (link 9.) is het gebruik van add-ons om fingerprinting tegen te gaan al eens aan de orde gekomen. De tijd heeft echter niet stilgestaan en er is wel het een en ander gewijzigd. Dus een opfrisser kan geen kwaad.

Allereerst gaan we de configuratie aanpassen en daarna add-ons toevoegen. Firefox ondersteunt *DNS over HTTPS*. Dit gaan we het eerst instellen. We gaan naar: *Instellingen* > *Algemeen* > *Netwerkinstellingen* > *DNS over HTTPS* inschakelen. Bij *Provider gebruiken* kiezen we *Aangepast* en vullen in: *dns.quad9.net/dns-query*. Verder zorgen we uiteraard dat we automatisch updates krijgen.

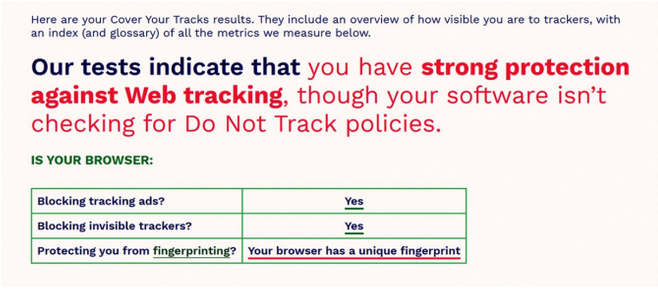
Bij *Startpagina* kiezen we een *Lege pagina* bij zowel *Startpagina en lege vensters*, als *Nieuwe tabbladen*.
Bij *Zoeken* kiezen we als veilige zoekmachine *DuckDuckGo* en halen het vinkje weg bij *Zoeksuggesties geven*. Met het laatste bereiken we dat er zo min mogelijk informatie naar de zoekmachineserver wordt gestuurd.

We gaan nu naar *Privacy & Beveiliging*. Bij *Verbeterde bescherming tegen volgen selecteren* we *Streng*. Er wordt gewaarschuwd dat sommige websites niet zouden kunnen werken. In de praktijk valt dat erg mee en anders, als het gebeurt, even op *Standaard* zetten. Vinkjes bij *Cookies en websitegegevens verwijderen zodra Firefox wordt gesloten*, *Waarschuwingen over wachtwoorden voor getroffen websites tonen*, *Pop-upvensters blokkeren* en *Waarschuwen wanneer websites add-ons proberen te installeren*. Bij *Firefox-gegevensverzameling en -gebruik* verwijderen we alle vinkjes. Bij *Beveiliging en Certificaten* zetten we vinkjes.
We selecteren verder *Alleen-HTTPS-modus in alle vensters inschakelen*. Nu zijn de add-ons aan de beurt. We gaan nu de volgende add-ons in de aangegeven volgorde installeren:

- Qwant lite;
- startpage.com Nederlands;
- Disconnect;
- uBlock origin;
- Privacy Badger;
- I don't care about cookies;
- temporary containers;
- webGL Fingerprint Defender.

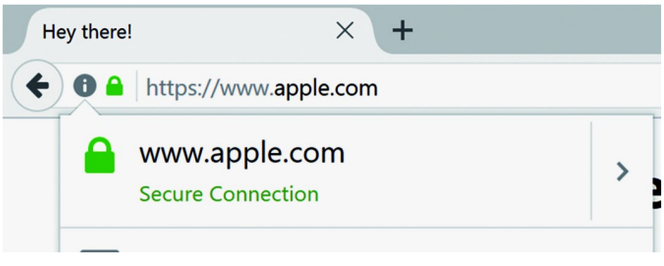
We voegen twee zoekmachines toe. *Qwant* is een Franse zoekmachine die privacy hoog in het vaandel heeft staan. Die maken we de standaard zoekmachine. Gezien de Europese privacywetgeving prefereer ik een Europese zoekmachine. *Startpage.com* is een Nederlandse zoekmachine met hoge privacystandaards die Google als zoekmachine gebruikt. Op deze manier kun je Google gebruiken zonder de nadelen. Het gebruik van de drie zoekmachines Qwant, DuckDuckGo en Startpage.com is dat jouw oude zoekacties niet worden gebruikt bij een nieuwe zoekactie. Daarmee voorkom je tunnelvisie. Je zoekt steeds met een open en frisse blik op internet.
Disconnect blokkeert bekende malware-sites. Dat lijkt een beetje overbodig omdat we *Quad9* gebruiken als DNS-server. Maar het kan geen kwaad.
De add-on *uBlock origin* blokkeert advertenties en *Privacy Badger* doet dat met onzichtbare links (zogenaamde pixel-links) naar ongewenste sites.
I don't care about cookies accepteert automatisch cookies en bevrijdt je van extra klikken.
Temporary containers zorgt ervoor dat ieder tabblad zijn eigen cookie-trommel krijgt. Op die manier weet een website

in een tabblad niets van het bezoek in het andere tabblad. Zet het op automatisch en verwijder eventuele vooraf ingestelde containers.
WebGL Fingerprint Defender pakt een set vingerafdrukken die Firefox laat liggen. Bij Firefox onder Linux blijkt die trouwens niet nodig te zijn.
Om te kijken wat nu het resultaat is van deze instellingen gaan we naar de pagina *Cover your tracks* van de website van *Electronic Frontier Foundation* (link 10). Als we alles goed hebben gedaan krijgen we als resultaat:



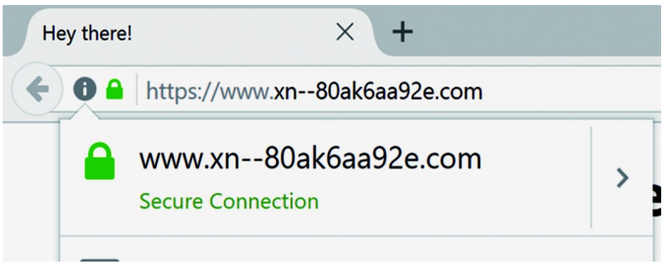
Afbeelding 4: Resultaat vingerafdruktest

Nu zul je denken: 'Ik ben uniek, dus makkelijk te volgen'. Niet dus. Na deze check wordt je vingerafdruk opgenomen in de database en voor een aantal maanden bewaard. Als je direct hierna de check weer doet ben je weer uniek. Dat is omdat er weer een nieuwe vingerafdruk is gegenereerd. Op deze manier wordt het juist lastiger om je te volgen: je bent steeds op een andere manier uniek.
Websitenamen zijn niet altijd wat ze lijken. Met het gebruik van *Punycode* (link 11) is geïntroduceerd dat Unicode-karakters worden weergegeven als ASCII-karakters. Dit heeft een veiligheidsprobleem veroorzaakt bij de weergave van websitenamen. De manier waarop browsers domeinnamen laten zien kan hierdoor verwarring geven. Een website kan een bekende domeinnaam laten zien. Als voorbeeld zie je hieronder hoe je kan worden misleid bij de meeste browsers.



Afbeelding 5: Apple als ASCII-code

Firefox kan hiertegen bescherming bieden. Om Firefox hiervoor aan te passen tik je in het URL-veld: *about:config*. Je komt dan bij de geavanceerde configuratievoorkeuren van Firefox. Hiermee moet je voorzichtig omgaan. Je kunt namelijk veel vernietigen. Vandaar dat je een waarschuwing krijgt. Klik op: *Het risico aanvaarden en doorgaan*. Tik daarna in het zoekveld *puny* in.
Je vindt: *network.IDN_show_punycode* met daarachter *false*. Dubbelklik op false; dan wordt het true. Vanaf nu zie je de *punycode* van domeinnamen. De hierboven getoonde website laat nu zijn ware naam zien.



Afbeelding 6: Apple als punycode

We zien dat **xn--80ak6aa92e.com** zich voordoet als **apple.com**. Het is u duidelijk dat dit een poging tot phishing is.

De mailclient

Hoewel er in de loop van de tijd andere communicatiemogelijkheden bij zijn gekomen, gebruiken we allemaal nog wel onze mail. Outlook is de standaard mailclient in Windows. Omdat ik in Linux Thunderbird gebruik, heb ik hier bij Windows ook voor gekozen.
Ik vind dat plezieriger dan twee verschillende mailclients gebruiken. Zie voor overstappen op Thunderbird: SoftwareBus 2017-2 (link 12.) Ook te vinden op de site op: **https://www.compusers.nl/inhoud-softwarebus-2017-2** (wel eerst inloggen).

De veiligheid bij mail is nog ver te zoeken; je mail is niet versleuteld. Wel is, mits je de juiste instellingen gebruikt, de verbinding naar de mailserver versleuteld. Verkeer tussen mailservers is niet altijd versleuteld. Als de zender en de ontvanger de juiste instellingen hebben, zal dat wel het geval zijn, maar daar is helaas geen garantie op. Ook is je mail op de mailserver niet versleuteld. Het gebruik van versleutelde mail kan alleen als beide zijden daar afspraken over hebben gemaakt. Dit gaat echter te ver voor dit artikel.

Voor het instellen van Thunderbird gaan we naar *Extra* > *Opties* > *Algemeen* en stellen we als standaard zoekmachine *DuckDuckGo* in en bij *Verbindingsinstellingen* > *DNS over HTTPS inschakelen*: *Aangepast voor dns.quad9.net/dns-query.*

Nu gaan we naar: *Extra* > *Opties* > *Privacy & Beveiliging*. We halen het vinkje weg bij *Externe inhoud in berichten toestaan*. En een vinkje bij *Cookies van websites accepteren* we. Bij *Cookies van derden accepteren* halen we het vinkje weg.

We bewaren de cookies tot Thunderbird wordt afgesloten. We zetten een vinkje bij het *'Niet volgen'*-signaal en zetten *ongewenste berichten* op zelflerend. Bij *Thunderbird-gegevensverzameling en gebruik* halen we alle vinkjes weg. *Scamdetectie* zetten we aan en anti-virusprogramma's geven we toestemming om inkomende berichten in quarantaine te zetten.

Bij het afhandelen van inkomende mail moeten we opletten of het geen poging tot phishing is. Dus we moeten voorzichtig zijn bij berichten van onbekenden, maar ook bij mails van banken. Als we twijfelen moeten we de broncode bekijken. Daarvoor zet je bij *Postvak in* de cursor op het betreffende bericht. Daarna gaan we naar: *Beeld* > *Berichtbron*. Je krijgt dan extra informatie te zien van het bericht.

Als voorbeeld laat ik een deel zien van een bericht dat ik zogenaamd van *Mijn Overheid* kreeg. In dit bericht werd mij gevraag om i.v.m. een storing op een link in dit bericht te klikken. Je ziet echter dat het echte mailadres van de zender niet van *Mijn Overheid* is (afbeelding 7). Dit is dus een duidelijke poging tot phishing.

Afbeelding 7: Broncode van 'Mijn Overheid'

De cloud

Moeten we nu wel of niet de cloud gebruiken? Deze vraag stellen roept soms heftige discussies op. Ik hoop dus dat ik geen olie op het vuur gooi. De zo genoemde 'cloud' is niet altijd een cloud. Vaak is het een enkele server. Bij de cloud weet u namelijk niet waar de gegevens worden opgeslagen. De cloud is namelijk een verzameling van servers waarop de gegevens kunnen staan. Dus ook in landen waar je niet wilt dat jouw gegevens staan.
Denk eraan dat zelfs versleutelde gegevens te ontsleutelen zijn. Dat is slechts een kwestie van tijd. Met lange sleutels maak je het wel moeilijker, maar ik denk dat er maar weinig mensen zijn die sleutels van meer dan 32 karakters gebruiken. Gratis clouds zou ik nooit gebruiken. De vraag is dan namelijk wat het verdienmodel is van de leverancier. Dat kan het verzamelen en verkopen van je gegevens zijn. Een betaalde cloud gebruiken met een zakelijk contract, waarin afgesproken is dat de gegevens binnen de EU zijn opgeslagen, vind ik acceptabel. Clouds voor de gewone consument – zelfs betaalde – raad ik ten sterkste af. Daar is weinig garantie dat de gegevens binnen de EU blijven. Er zijn trouwens ook EU-landen waar je je vraagtekens bij kunt zetten.
Dit geldt natuurlijk ook voor de mailserver die je gebruikt.

Camera en microfoon

De camera en microfoon zijn belangrijk geworden nu we zoveel via internet regelen. In sommige laptops kun je in het BIOS de camera uitschakelen. Als je de camera niet of weinig gebruikt raad ik dit aan. In andere gevallen: doe een klepje voor het objectief als je hem niet gebruikt. Een kartonnetje werkt ook prima. Verder is het verstandig om de toegang van programma's tot camera en microfoon te beperken. Geef alleen programma's die het echt nodig hebben toegang. Je kunt dat instellen bij *Instellingen* > *Privacy*. Als je hier toch bezig bent, schakel dan ook *Locatie* uit.
De beste beveiliging is natuurlijk een fysieke, want software kan altijd worden gekraakt.

Conclusie

Door aandacht te besteden aan de instellingen van Windows, de browser en de mailclient kun je de privacy en beveiliging aanzienlijk verbeteren. Het is echter geen gelopen race. Je zal hier steeds aandacht aan moeten besteden; de onverlaten zitten namelijk niet stil. Een gezond wantrouwen kan nooit kwaad.

Links

1. https://www.xda-developers.com/windows-11-microsoft-local-account/
2. https://www.safer-networking.org/products/spybot-anti-beacon/
3. https://www.compusers.nl/system/files/swb-jaargangen/2021/2021-4/SwB20214_Veilig(er)_internet_(2).pdf
4. https://www.simplednscrypt.org/
5. https://www.quad9.net/
6. https://www.av-test.org/en/
7. https://www.zonealarm.com/software/free-firewall/
8. https://www.f-secure.com/nl/home
9. https://www.compusers.nl/sites/default/files/swb-jaargangen/2019/2019-3/SwB20193_Blokkeer_fingerprinting.pdf
10. https://coveryourtracks.eff.org/
11. https://en.wikipedia.org/wiki/Punycode
12. https://www.compusers.nl/sites/default/files/swb-jaargangen/2017/2017-2/SwB20172_Overstappen-naar-Thunderbird.pdf