TOON VAN DAELE | **NIVEAU** ●○○○○

MICROSOFT DEFENDER GEBRUIKEN

Een virusscanner is noodzakelijk op elke computer die met het internet is verbonden. Precies zo'n scanner is in Windows 10 en 11 ingebouwd: Microsoft Defender. Hoe ga je hiermee om?

Er circuleert behoorlijk wat schadelijke software, oftewel malware, die zowel Windows als je persoonlijke bestanden kan aantasten. Gelukkig bestaan er antivirustools die dergelijke malware kunnen tegenhouden en neutraliseren, zoals Norton, McAfee, Avast of Bitdefender. Echter, het ingebouwde en kosteloze antivirusprogramma van Windows, Microsoft Defender, is eigenlijk net zo effectief. Je hebt dus weinig te vrezen, vooral als je geen (illegale) software uit dubieuze bronnen installeert, geen verdachte websites bezoekt en nooit lukraak op links van onbekende afzenders klikt.

1 AUTOMATISCH

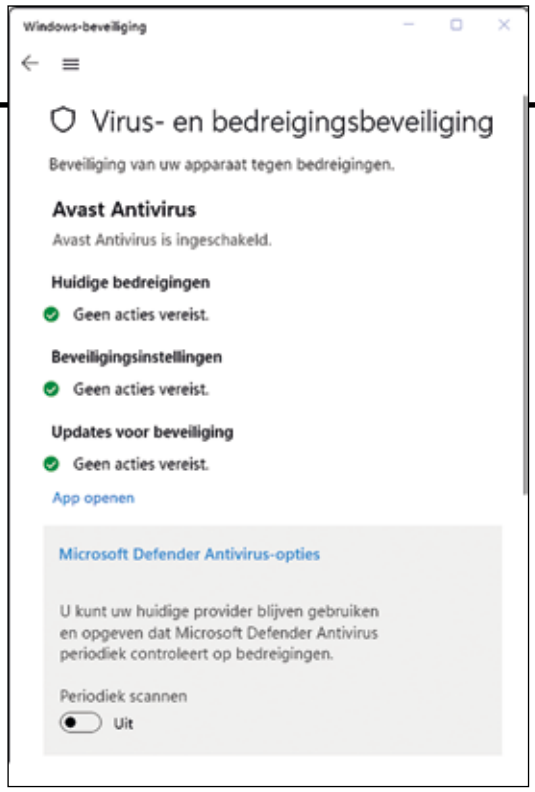
Microsoft Defender wordt automatisch ingeschakeld en werkt op de achtergrond, waardoor je er in principe zelf niets aan hoeft te doen. Deze *tool* vraagt zelden om jouw inbreng, tenzij het echt nodig is, bijvoorbeeld bij het detecteren van een virus of andere bedreiging. Let wel, Microsoft Defender wordt automatisch uitgeschakeld wanneer je een extern antivirusprogramma installeert, omdat twee dergelijke tools op de achtergrond elkaar kunnen tegenwerken. Zodra je de externe antivirustool verwijdert, zal Microsoft Defender zichzelf weer inschakelen.

2 VINKJE

Om er zeker van te zijn dat de antivirus-service actief is, open je het Windows-startmenu, druk je op *Instellingen* en navigeer je naar *Bijwerken en beveiliging* (Windows 10) of *Privacy en beveiliging* (Windows 11), waar je *Windows-beveiliging* opent. Je ziet op de afbeelding hierboven dat de ingebouwde beveiliging uit meerdere onderdelen bestaat, maar we richten ons hier enkel op het onderdeel *Virus- en bedreigingsbeveiliging*. Als hier een groen vinkje staat (dus geen kruis op een rode achtergrond), betekent dit dat er een actieve antivirusbescherming is, en dat is waar we voorlopig van uitgaan.

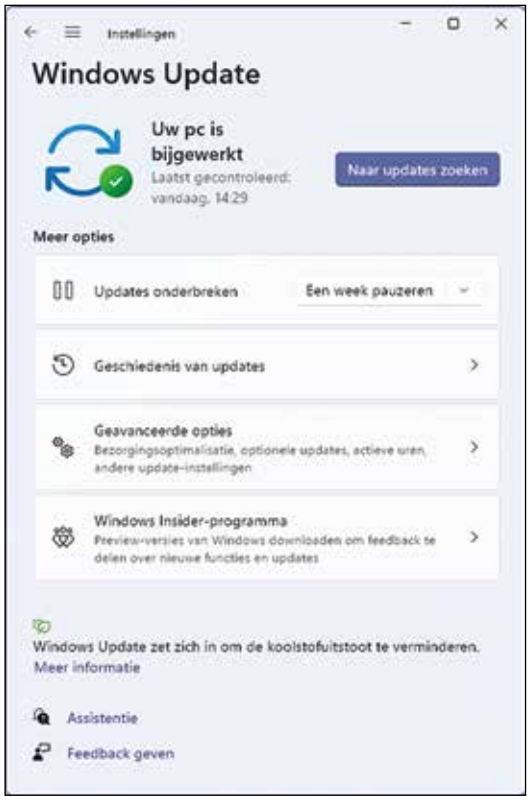
3 PERIODIEKE SCAN

Klik hier op *Virus- en bedreigingsbeveiliging*. Als je eerder een ander antivirusprogramma hebt geïnstalleerd, zie je hier de naam van die tool. Defender is niet langer actief op de achtergrond, maar je kunt ervoor kiezen om het af en toe een virusscan uit te laten voeren. Klik hiervoor op *Microsoft Defender Antivirus-opties* en schakel *Periodiek Scannen* in door de knop op *Aan* te zetten en te bevestigen met *Ja*.
In dit artikel gaan we er verder wel van uit dat Defender je enige antivirusprogramma is.



4 UPDATES

In de introductie van dit artikel hebben we al besproken waar je op moet letten om kwaadaardige software te vermijden. Om Defender efficiënt te kunnen gebruiken, is het evenwel ook belangrijk dat de tool zichzelf altijd kan updaten. Dit gebeurt in principe automatisch, samen met andere Windows-updates, maar het kan geen kwaad af en toe te controleren of deze functie voor automatische Windows-updates wel is ingeschakeld. Ga hiervoor terug naar *Instellingen* en selecteer *Windows Update*. Klik indien van toepassing op



Updates hervatten of *Naar updates zoeken*. Als alles in orde is, verschijnt (mogelijk na het installeren van beschikbare updates) de melding 'Uw pc is bijgewerkt'. Je hoeft verder niets te doen en kunt erop vertrouwen dat Microsoft Defender up-to-date wordt gehouden.

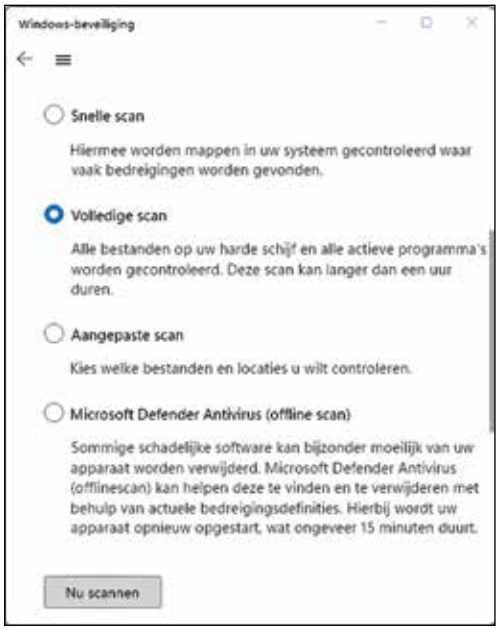
5 SNELLE SCAN

Prima, Defender is actief en up-to-date. We leggen zo uit wat er gebeurt als de tool iets verdachts detecteert. Eerst laten we je zien hoe je zelf een virusscan kunt uitvoeren. Hoewel dit in principe niet nodig is, aangezien de tool continu op de achtergrond werkt, kan het geen kwaad om het te doen. Ga hiervoor terug naar *Virus- en bedreigingsbeveiliging* en klik op de knop *Snelle scan*. De scan begint direct en duurt enkele minuten. Wel kun je op elk moment op de knop *Annuleren* drukken. Voorlopig gaan we ervan uit dat het resultaat helemaal naar wens is en de melding 'Geen acties vereist' verschijnt.

6 ANDERE SCANS

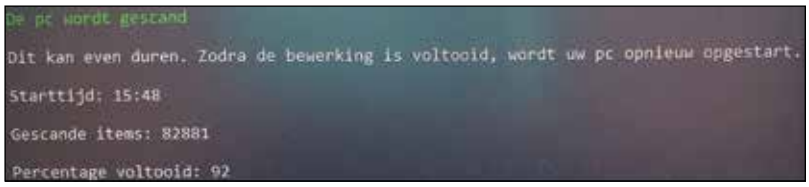
Het kan voorkomen dat een snelle scan je niet volledig geruststelt, bijvoorbeeld als je computer vreemd gedrag vertoont. In dat geval kun je kiezen voor een grondigere scan. Klik hiervoor op *Scanopties* waardoor meer scantypes beschikbaar worden, waaronder *Volledige scan*. Selecteer deze en klik op *Nu scannen*. Defender controleert hierbij alle bestanden op je pc, wat aanzienlijk langer kan duren, tot wel een uur of meer.

Als je een specifieke map in gedachten hebt met mogelijk verdachte bestanden – zoals recente downloads – kun je in plaats daarvan een *Aangepaste scan* selecteren. Wanneer je op *Nu scannen* klikt, verschijnt een bestandsverkenner en kun je zelf de map kiezen die Defender op mogelijke malware moet controleren. Je kunt zo'n scan overigens ook vanuit de Verkenner uitvoeren. Klik met de rechtermuisknop op een map en kies *Scannen met Microsoft Defender*. ▶



7 OFFLINE SCAN

Als een volledige scan geen verdachte zaken oplevert, is de kans dat er schadelijke software op je systeem staat klein, maar je kunt dit nooit volledig uitsluiten. Mocht je toch het vermoeden hebben van een virusinfectie – aangezien er inderdaad malware bestaat die zich diep in het systeem verbergt en daardoor niet altijd gedetecteerd wordt door 'gewone' scans (ook niet van andere antivirusprogramma's) – dan kun je altijd nog kiezen voor de optie Microsoft Defender Antivirus (offline scan).



Zodra je op *Nu scannen* klikt en het scannen bevestigt met *Ja*, zal je computer opnieuw opstarten en direct daarna je systeem scannen, voordat Windows en eventuele malware de kans krijgen om op te starten. Zorg er dus wel voor dat je eerst alle programma's sluit en geopende documenten veilig opslaat.

8 BEDREIGINGSMELDING

Wanneer Defender een mogelijke bedreiging detecteert, ontvang je direct een notificatie in het meldingencentrum. Dit open je met de sneltoets *Windows-toets + N* of door op de datum en tijd te klikken, die rechts op de Windows-taakbalk staat. Als er meer meldingen zijn, klik je eventueel op *+[n] meldingen*. Door op een bedreigingsmelding te klikken, opent automatisch het onderdeel *Virus- en bedreigingsbeveiliging*, maar je kunt dit ook altijd handmatig openen. Als je hier bij *Huidige bedreigingen* niets ziet, klik dan op *Beveiligingsgeschiedenis*, zodat hier de meest recent vastgestelde bedreigingen worden weergegeven.

9 INFORMATIE

Bij elke gedetecteerde bedreiging krijg je een inschatting van het risico volgens Microsoft, zoals *Ernstig*, *Hoog* en *Laag*. Je krijgt ook een korte beschrijving van eventuele acties die je eerder hebt ondernomen met betrekking tot deze bedreiging, zoals *Oplossing onvolledig*, *Mogelijk ongewenste app gevonden* of *Bedreiging toegestaan*.
Klik op de betreffende melding. Voor aanvullende informatie, zoals de exacte locatie van het bestand op je computer, kun je vervolgens op *Details weergeven* klikken.
In dit venster vind je doorgaans ook de optie *Meer informatie*. Deze link brengt je naar een Microsoft-website met extra feedback, zoals typische symptomen en de beste manier om te reageren.

10 ACTIES

In dit venster kun je tevens aangeven welke actie je wilt ondernemen tegen deze bedreiging. Er zijn drie opties: *Verwijderen*, *Quarantaine* en *Toestaan op apparaat*.
De eerste spreekt voor zich: hiermee verwijder je het verdachte bestand van je computer. Kies deze actie en bevestig met *Acties starten*.

De derde optie is het 'tegenovergestelde': je geeft aan dat je het bestand vertrouwt en laat Defender weten dat het voortaan genegeerd mag worden. Dit is handig als je een app hebt gedownload waarvan je weet dat deze veilig is, maar die door Microsoft als potentieel verdacht wordt beschouwd, zoals een tool om productsleutels of wachtwoorden te achterhalen.

11 IN QUARANTAINE

Het kan voorkomen dat je vermoedt dat een bestand onschadelijk is, terwijl Microsoft het niet volledig vertrouwt. Het bestand direct verwijderen is misschien zonde, maar het zonder meer toestaan brengt risico's met zich. In zo'n situatie kun je kiezen voor de tweede optie: *Quarantaine*. Wanneer je bevestigt met *Acties starten*, plaatst Defender het bestand in een veilige locatie waar zelfs een kwaadaardig bestand geen schade kan aanrichten. Zodra je voldoende informatie hebt

verzameld die aantoont dat het bestand betrouwbaar is, kun je het alsnog uit quarantaine halen.

12 UIT QUARANTAINE

Om een bestand uit quarantaine te halen, volg je de volgende stappen. Ga naar *Virus- en bedreigingsbeveiliging* en selecteer *Beveiligingsgeschiedenis*. Klik eventueel op *Filters* en kies *Items in quarantaine*. Selecteer het item dat je wilt bewaren en klik op *Herstellen*. Het bestand keert dan terug naar de locatie waar het zich bevond voordat Defender het in quarantaine plaatste.
Het tegenovergestelde is ook mogelijk: door *Verwijderen* te kiezen, wordt het bestand definitief gewist. Als je eerder te snel *Toestaan* had geselecteerd en daar nu spijt van hebt omdat het bestand bij nader inzien toch verdacht blijkt, klik dan op *Toegestane bedreigingen*, selecteer het betreffende item en kies *Niet toestaan*.

13 UITSCHAKELEN

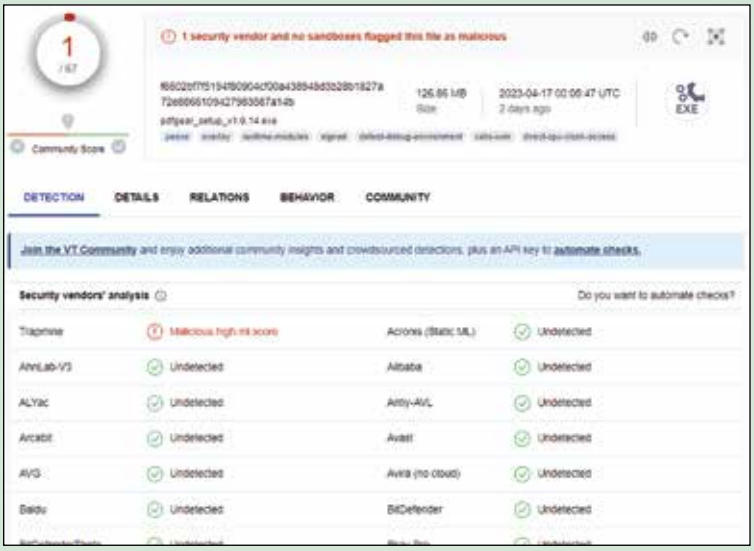
Het kan wel eens voorkomen dat Defender zo koppig is dat je er niet in slaagt een (programma) bestand, waarvan je weet dat het onschadelijk is, te downloaden of te installeren. In dit uitzonderlijke geval kun je overwegen om Defender tijdelijk uit te schakelen.

Dit doe je via *Virus- en bedreigingsbeveiliging*, waar je bij *Instellingen voor Virus- en bedreigingsbeveiliging* op *Instellingen beheren* klikt. Zet vervolgens de schakelknop bij *Realtime-beveiliging* (lees: automatische virusbescherming op de achtergrond) op *Uit* en bevestig met *Ja*. Er verschijnt nu een melding dat de bescherming niet langer intact is.
Na de download of installatie kun je Defender meteen weer inschakelen door de schakelknop op *Aan* te zetten. Je kunt ook je pc opnieuw opstarten, want dan zorgt Windows er normaal gesproken voor dat Defender vanzelf weer wordt ingeschakeld.

NIVEAU ●●○○○

VirusTotal

Hoewel Defender een betrouwbare antivirusoplossing is die automatisch gedownloade bestanden controleert, kan het geen kwaad om extra voorzorgsmaatregelen te nemen. Voordat je recent gedownloade bestanden opent of start, kun je ze naar de gratis online antivirusdienst VirusTotal (www.virustotal.com) sturen voor een aanvullende check.
Klik hier op *Choose file* en selecteer het betreffende bestand.
Even later verschijnt een lijst met scanresultaten van vaak 70 of meer antivirustools. Het kan gebeuren dat enkele antivirusprogramma's een mogelijke bedreiging detecteren in het geüploade bestand. Echter, als slechts twee of drie (voornamelijk onbekende) programma's een bedreiging aangeven, kun je er doorgaans van uitgaan dat het bestand veilig is. Als er meer programma's een bedreiging signaleren, wees dan extra voorzichtig!



14 INSTELLINGEN

Blijf even bij *Instellingen beheren*, want je treft hier diverse andere opties aan, zoals *Cloudbeveiliging* en *Automatisch sample indienen*. Het is aanbevolen om beide opties ingeschakeld te houden, aangezien dit betere *realtime* bescherming biedt. Defender kan bij twijfel dan een bestand naar de cloud sturen voor een snelle en up-to-date analyse. Laat ook *Manipulatiebescherming* ingeschakeld, want deze functie voorkomt ongewenste wijzigingen in je beveiligingsinstellingen. Meer informatie vind je op https://tinyurl.com/pca-cloudbeveiliging.
Daarnaast is er onder meer de optie *Uitsluitingen toevoegen of verwijderen*. Met *+Een uitsluiting toevoegen* kun je eventueel bestanden aan een *whitelist* toevoegen, waardoor Defender deze niet meer controleert. Om een bestand uit deze lijst te halen, klik je erop en kies je *Verwijderen*. ■