

Windows bijlage in nieuwsbrief 8

Auteur: Christ Flinsenberg



Inhoud Bijlage nieuwsbrief 8



Windows beveiliging

- Algemeen
- Scanopties
- Geavanceerde instellingen
- Firewall- en netwerken beveiliging

Cloudopslag

- Algemeen
- Beveiligingsaspecten met de Cloud

Beveiliging Algemeen

(1)



De beveiliging in Windows 10 is sterk verbeterd t.o.v. een paar jaar geleden. In deze bijlage bekijken we de standaard beveiligingsopties die in Windows 10 aanwezig zijn.

We behandelen geen aparte beveiligingspakketten die te koop of gratis te downloaden zijn.

Maar Windows 10 werkt samen als er een apart beveiligingspakket is geïnstalleerd.

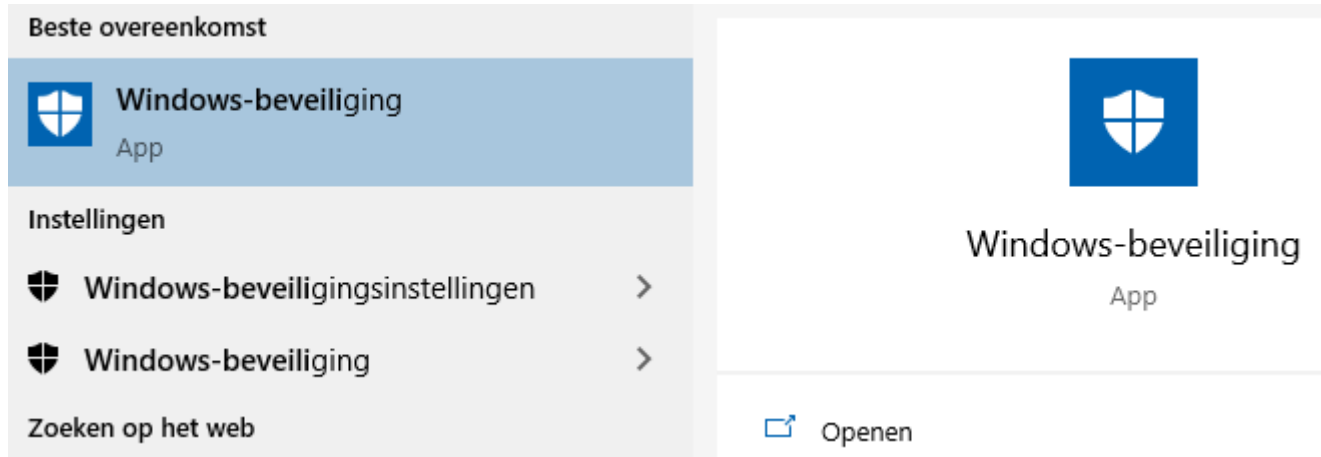
Windows-beveiliging

(1)



Alles wat met beveiliging te maken heeft, vind je in het onderdeel Windows-beveiliging.

Tik in zoek pictogram “windows-beveiliging” en je kunt de App Windows-beveiliging openen



Windows-beveiliging

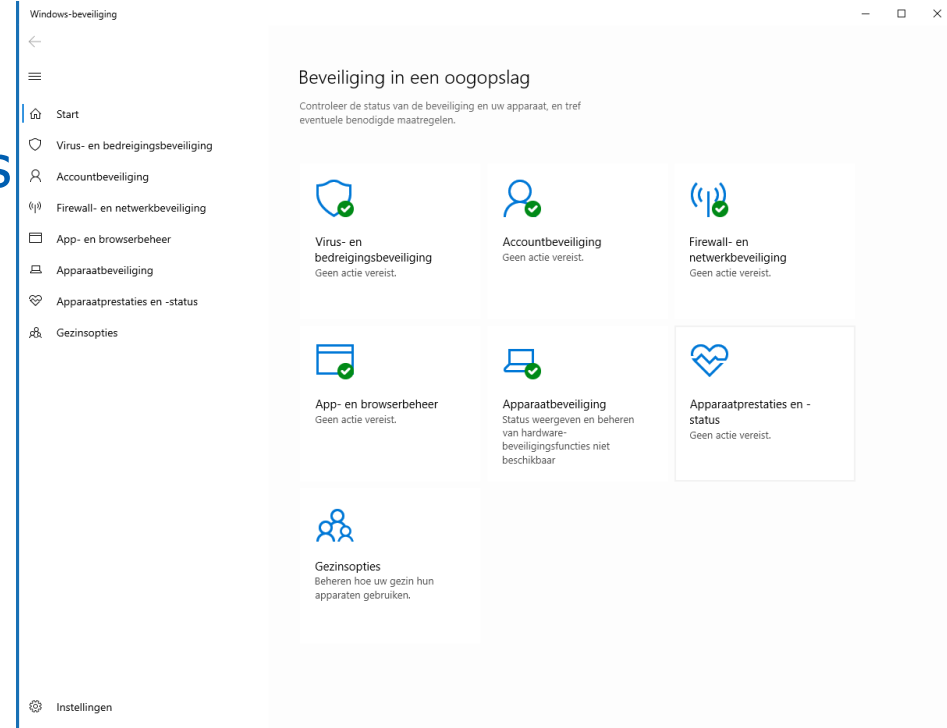
(2)



Het onderdeel Windows-beveiliging wordt weergegeven en je krijgt een overzicht te zien van diverse functies

De blauwe pictogrammen komen overeen met de opties in het menu.

Als je in dit scherm alleen maar groene vinkjes ziet, dan zijn er geen gevaren gevonden of virussen gedetecteerd.



Windows-beveiliging

(3)



Onderdeel Virus- en bedreigingsbeveiliging (Windows Defender)

- Status beveiliging
- Informatie virusdefinitie
- Laatste uitgevoerde scan

The screenshot shows the Windows Defender application window. The left sidebar contains a navigation menu with the following items: Start, Virus- en bedreigingsbeveiliging (selected), Accountbeveiliging, Firewall- en netwerkbeveiliging, App- en browserbeheer, Apparaatbeveiliging, Apparaatprestaties en -status, and Gezinsopties. The main content area is titled 'Virus- en bedreigingsbeveiliging' and displays the following information:

- Virus- en bedreigingsbeveiliging**: Beveiliging van uw apparaat tegen bedreigingen. Includes a link to 'Video's van de Windows-community's' and 'Meer informatie over Virus- en bedreigingsbeveiliging'.
- Huidige bedreigingen**: Momenteel geen bedreigingen. Laatste scan: 2-1-2020 15:18 (snelle scan). 0 bedreigingen gevonden. Scan heeft 7 minuten 57 seconden geduurd. 29946 bestanden gescand. Includes a 'Snelle scan' button and links for 'Scanopties', 'Toegestane bedreigingen', and 'Beschermingsgeschiedenis'.
- Instellingen voor virus- en bedreigingsbeveiliging**: Geen actie vereist. Includes a link for 'Instellingen beheren'.
- Updates van virus- en bedreigingsbeveiliging**: Security Intelligence is up-to-date. Laatste update: 3-1-2020 09:14. Includes a link for 'Controleren op updates'.
- Bescherming tegen ransomware**: Geen actie vereist. Includes a link for 'Bescherming tegen ransomware beheren'.

At the bottom left of the window, there is a link for 'Instellingen'.

Windows-beveiliging

(4)



Scan mogelijkheden:

- Snelle scan
- Volledige scan
- Aangepaste scan
- Windows Defender Offline-scan

De laatste optie kan interessant zijn, als je het vermoeden hebt dat er hardnekkige malware op de computer aanwezig is.

Doe deze laatste methode niet als je ondertussen iets anders aan het doen bent.

Snelle scan

Hiermee worden mappen in uw systeem gecontroleerd waar vaak bedreigingen worden gevonden.

Volledige scan

Alle bestanden op uw harde schijf en alle actieve programma's worden gecontroleerd. Deze scan kan langer dan een uur duren.

Aangepaste scan

Kies welke bestanden en locaties u wilt controleren.

Windows Defender Offline-scan

Bepaalde schadelijke software kan soms moeilijk van uw apparaat worden verwijderd. Windows Defender Offline gebruikt bijgewerkte bedreigingsdefinities om deze schadelijke software beter te kunnen vinden en verwijderen. Dit proces duurt ongeveer 15 minuten en uw apparaat wordt hiervoor opnieuw opgestart.

Nu scannen

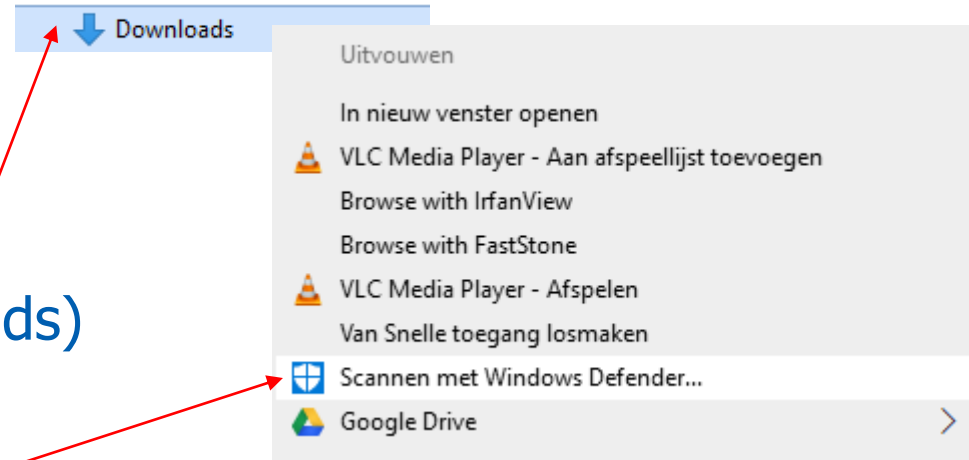
Windows-beveiliging

(5)



Windows Defender is volledig geïntegreerd in Windows 10, hierdoor kun je de scan-opties ook vanuit de Verkenner benaderen.

Wil je een bepaalde map of programma scannen. Klik met de rechtermuisknop op de des betreffende map (hier Downloads) Kies in het contextmenu de optie Scannen met Windows Defender...



Windows-beveiliging

(6)



Onder Instellingen voor virus- en bedreigingsbeveiliging kun je een aantal geavanceerde instellingen wijzigen

The screenshot shows the Windows Security application window. The title bar reads 'Windows-beveiliging'. The main content area is titled 'Virus- en bedreigingsbeveiliging' and contains the following sections:

- Virus- en bedreigingsbeveiliging**: Beveiliging van uw apparaat tegen bedreigingen.
- Huidige bedreigingen**: Momenteel geen bedreigingen. Laatste scan: 3-1-2020 17:23 (snelle scan) 0 bedreigingen gevonden. Scan heeft 8 minuten 10 seconden geduurd. 28397 bestanden gescand. A 'Snelle scan' button is visible.
- Instellingen voor virus- en bedreigingsbeveiliging**: Geen actie vereist. A red box highlights the 'Instellingen beheren' link.

The right sidebar contains several links and options:

- Video's van de Windows-community's: [Meer informatie over Virus- en bedreigingsbeveiliging](#)
- Hebt u een vraag?: [Hulp vragen](#)
- Wie beschermt mij?: [Providers beheren](#)
- Windows-beveiliging helpen verbeteren: [Feedback geven](#)
- Uw privacy-instellingen wijzigen: [Bekijk en wijzig de privacy-instellingen voor uw Windows 10-apparaat.](#)

The left navigation pane includes: Start, Virus- en bedreigingsbeveiliging (selected), Accountbeveiliging, Firewall- en netwerkbeveiliging, App- en browserbeheer, Apparaatbeveiliging, Apparaatprestaties en -status, and Gezinsopties.

Realtime-beveiliging

Realtime beveiliging zorgt ervoor dat Windows Defender altijd actief is op de achtergrond en dus actief gevaarlijke bestanden blokkeert en direct verwijdert. Als je deze optie uitschakelt, wordt deze automatisch na verloop van tijd ingeschakeld.

Cloudbeveiliging

De naam is misschien wat misleidend, want het lijkt alsof jouw cloud (bijvoorbeeld OneDrive) wordt beveiligd, maar dat is dus niet zo. Microsoft haalt extra gegevens over virusdefinities en bekende beveiligingsproblemen uit de cloud als deze is ingeschakeld.

Automatisch sample indienen

Als deze optie is ingeschakeld worden bestanden die door Windows Defender aangemerkt zijn als gevaarlijk, automatisch naar Microsoft gestuurd voor analyse.

Manipulatiebescherming

Dit is een extra beveiliging die moet voorkomen dat onderdelen van Windows Defender op de achtergrond met een commando, bijvoorbeeld vanuit malware, kunnen worden uitgeschakeld, bijvoorbeeld via aanpassing in het register.

Controlled folder access

Deze optie zorgt ervoor dat bepaalde mappen op je computer, welke dat zijn kun je zelf instellen, extra worden beveiligd en gecontroleerd op ongeoorloofde toegang. Bijvoorbeeld in het geval van ransomware. De functie is standaard uitgeschakeld. Als je deze inschakelt, krijg je toegang tot geavanceerde instellingen. Windows mappen worden altijd beveiligd, maar je kunt ook extra mappen toevoegen.

Controlled folder access

Bescherm bestanden, mappen en geheugengebieden op uw apparaat tegen onbevoegde wijzigingen door schadelijke toepassingen.

Aan

[Geschiedenis van blokkeringen](#)

[Beschermd mappen](#)

[Een app toestaan via Controlled Folder Access](#)

Let op!!

Als je Controlled folder access hebt ingeschakeld dan kan het zijn dat een bepaald programma niet meer werkt.

Als voorbeeld. Ik heb Adobe Elements 2018 en als ik een verandering in een foto had aangebracht en deze daarna wilde opslaan, deed het programma dit niet. Toen ik bij de Controlled folder access ging kijken, bleek dat deze app werd geblokkeerd. Dit wil ik niet!!

Om dit aan te passen:

Windows-beveiliging

(11)



- Klik op 'Een app toestaan via Controlled Folder Access'
- Klik op Toestaan wijziging

Controlled folder access

Bescherm bestanden, mappen en geheugengebieden op uw apparaat tegen onbevoegde wijzigingen door schadelijke toepassingen.



[Geschiedenis van blokkeringen](#)

[Beschermd mappen](#)

[Een app toestaan via Controlled Folder Access](#)

Een app toestaan via Controlled Folder Access

Als Controlled Folder Access een app heeft geblokkeerd die u vertrouwt, kunt u deze app toevoegen als een toegestane app. Daardoor kan de app wijzigingen in beschermde mappen aanbrengen.

+ Een toegestane app toevoegen

Windows-beveiliging

(12)



- Je kunt kiezen uit Onlangs geblokkeerde apps of 'Door alle apps bladeren'.
- Ik kies voor eerste
- Klik op + teken bij de app die je wilt toestaan
- Deze worden nu in lijstje toegevoegd

Onlangs geblokkeerde apps

De volgende apps zijn onlangs geblokkeerd door gecontroleerde mappentoeegang. Zorg ervoor dat u een app vertrouwt voordat u deze toestaat.

+	PremiereElementsEditor.exe C:\Program Files\Adobe\Adobe Premiere Elements 2018\PremiereElementsEditor.exe 16-10-2020 09:56
+	googledrivesync.exe C:\Program Files\Google\Drive\googledrivesync.exe 2-10-2020 09:29
+	Au_.exe C:\Users\Christ Flinsenbergh\AppData\Local\Temp\~nsuA.tmp\Au_.exe 1-10-2020 16:38
+	PhotoshopElementsEditor.exe C:\Program Files\Adobe\Photoshop Elements 2018\PhotoshopElementsEditor.exe 11-9-2020 10:56
	undaterrcorehelner.exe

[Door alle apps bladeren](#)

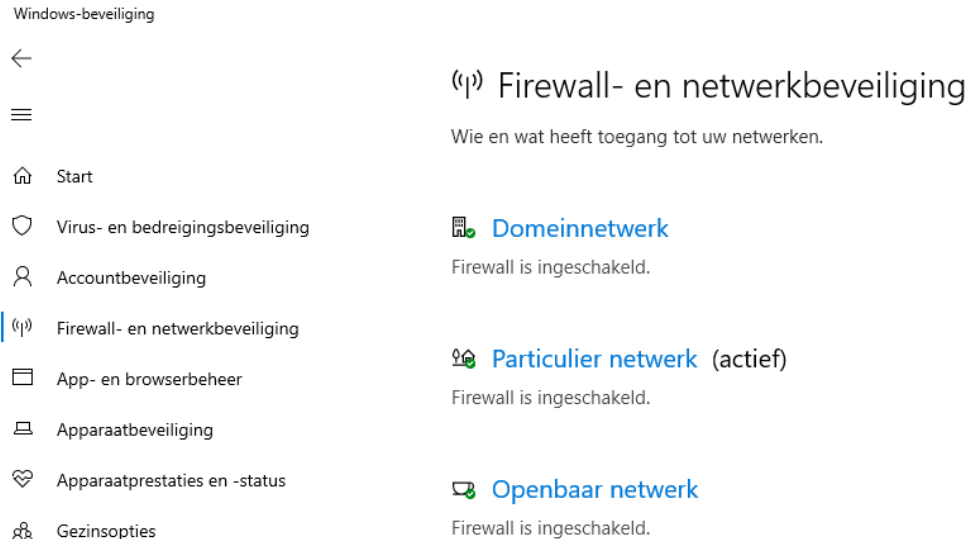
Sluiten

PremiereElementsEditor.exe
C:\Program Files\Adobe\Adobe Premiere Elements 2018

PhotoshopElementsEditor.exe
C:\Program Files\Adobe\Photoshop Elements 2018

Firewall- en netwerkbeveiliging

De Windows-firewall is onderdeel van de Windowsbeveiliging en zorgt ervoor dat je internetverbinding en je netwerk goed beveiligd is.



Windows-beveiliging

- ←
- ☰
- 🏠 Start
- 🛡️ Virus- en bedreigingsbeveiliging
- 👤 Accountbeveiliging
- | 🛡️ Firewall- en netwerkbeveiliging
- 📁 App- en browserbeheer
- 🖨️ Apparaatbeveiliging
- 💓 Apparaatprestaties en -status
- 👥 Gezinsopties

🛡️ Firewall- en netwerkbeveiliging

Wie en wat heeft toegang tot uw netwerken.

- 🌐 Domeinnetwerk
Firewall is ingeschakeld.
- 🏠 Particulier netwerk (actief)
Firewall is ingeschakeld.
- 🌐 Openbaar netwerk
Firewall is ingeschakeld.

Er zijn drie netwerkdelen:

Domeinnetwerk

Wanneer je computer is verbonden met een bedrijfsnetwerk, vind je in dit onderdeel de instellingen voor dit netwerk. Zelfs wanneer je computer geen verbinding heeft met een bedrijfsnetwerk, is dit onderdeel ingeschakeld.

Particulier netwerk

Dit kun je het beste omschrijven als je netwerk thuis. Ook deze beveiliging is standaard ingeschakeld

Openbaar netwerk

Een Openbaar netwerk wordt gezien als een netwerk buitenshuis of buiten het bedrijf. Denk aan een Wifi-verbinding in het café, op het vliegveld of in de trein. Ook deze bescherming is standaard ingeschakeld.

Windows Firewall schakelt alle netwerken automatisch in, zodat je overal daarvoor beveiligd bent.

Cloud opslag

Algemeen

(1)



Cloud opslag in het algemeen betekent dat gegevens, bestanden niet (alleen) op jouw computer staan, maar op een computer (server) van een bedrijf.

Dit wordt al jaren gedaan, denk hierbij aan Hotmail en Gmail, deze mails staan ook niet op jouw computer, maar bij Microsoft en Google.

Voorbeelden van cloudopslag: OneDrive, Google Drive en Dropbox.

Sinds een aantal jaren is het opslaan van bestanden in de cloud zowel privé als zakelijk enorm toegenomen.

Voordelen cloud opslag

- Kans op verlies door schade is zeer klein.
- Informatie blijft overal, waar internet verbinding is, bereikbaar.
- Veel cloud opslag bedrijven hebben deze applicaties voor computer, tablet en smartphone.
- Je kunt mappen of bestanden delen met anderen

Nadelen cloud opslag

- Privacy blijft een punt van aandacht.
- Eerste Giga bytes zijn gratis, voor meer opslag moet je betalen.
- Duurt langer (externe schijf sneller dan Wifi).

Beveiligingsaspecten met de cloud

(1)



Als je veel persoonlijke documenten en informatie in de cloud opslaat, zorg er dan voor dat je account goed beveiligd is. Hierbij moet u denken aan:

- Een sterk wachtwoord
- Pas 2 factor authenticatie toe als dit mogelijk is

Kies een wachtwoord met hoofdletters, kleine letters, cijfers en tekens en minimaal 10 karakters. Informatie over sterk wachtwoord zie bv. site <https://www.testjewachtwoord.nl>

Beveiligingsaspecten met de cloud

(2)



- Beveilig je apparaten tegen verlies of diefstal

Zorg dat de tablet of smartphone wordt vergrendeld als je het toestel niet gebruikt en gebruik een toegangscode.

- Algemene computer bescherming

Een virusscanner, firewall en Windows updates ingeschakeld.

Proclamatie



Alle informatie in deze documentatie is uitsluitend bedoeld voor eigen gebruik. Wij hebben er èrg veel tijd en energie in gestoken om dit te maken! Respecteer onze intellectuele eigendomsrechten en geef niets hiervan door aan anderen, als kopie of in welke vorm dan ook!

Stichting SeniorWeb Mierlo

