Bescherming in Windows 10

Rein de Jong

Uitgebreider beveiligd na de Fall Creators Update.

Onverlaten proberen op allerlei manieren zich toegang te verschaffen tot jouw digitale gegevens. Denk daarbij aan virussen, phishing en het ongeoorloofd gebruik maken van achterdeurtjes (exploits) die zich in software bevinden. Er zijn voortdurend wetenschappers, ethische hackers en criminelen op zoek naar de zwakke plekken. Vinden die laatsten een zwakke plek dan wordt dat uitgebuit. Aan de makers van antimalwareproducten de zware taak om de onverlaten een stap voor te zijn. Een bijgewerkte virusscanner alléén is onvoldoende. Naast het gebruik van een virusscanner is er de noodzaak van het regelmatig updaten van de producten en het maken van een versleutelde back-up op een veilige plek.[1]

Microsoft helpt ons, de gebruikers, via de beveiliging van Defender en het uitgeven van regelmatige updates, steeds beter bij het beschermen van onze digitale eigendommen. Met de komst van de herfstupdate van Windows 10, de 1709-versie, is de basisveiligheid in Windows 10 toegenomen. Er zijn functies toegevoegd die de veiligheid verhogen. Alleen zul je die wel eerst moeten vinden. Veel daarvan is aanwezig in de interface van Windows Defender. Die interface is voor sommigen helaas moeilijk te vinden. Daarnaast zijn er ook aanvullende beveiligingen, waarvoor je nog dieper in Windows moet duiken.
Windows Defender[2] is niet meer het basale antivirusprogramma dat het eerder was. Het wordt meer en meer volwassen. Het kan nog steeds niet de strijd aan met commerciële antivirusoplossingen[3]. Echter, wanneer je naast Defender ook nog een second opinionscanner, zoals HitManPro of MBAM, de pc wekelijks laat scannen, dan ben je voor normaal gebruik redelijk beveiligd en wordt je pc niet nodeloos vertraagd door een zware beveiliging. Een hotelportier passeer je immers ook sneller dan de beveiliging op Schiphol.

1 Extra in Windows 10

In Windows 10 (vanaf versie 1709) vinden we nieuwe mogelijkheden ter bescherming tegen malware. De mogelijkheid 'Beschermde mappen' wordt in het artikel uitgebreid belicht. Ook aan Exploit-bescherming besteed ik meer aandacht, omdat die ook via de interface van het Windows Defender-beveiligingscentrum in te stellen is. De andere beveiligingen, die alleen met Groepsbeleid of de PowerShell in te stellen zijn, zal ik beknopter beschrijven en bronnen aangeven waar meer informatie te vinden is. De voetnoten verwijzen naar de Engelstalige uitleg. Bedenk dat Groepsbeleid (GPedit.msc) alleen werkt in de Pro- en Enterprise-versie van Windows 10. De PowerShell werkt ook in de Homeversie.

1. **Beschermde mappen**[4]
   Dit wordt door Microsoft 'Controlled folder access' genoemd. Wanneer die functie goed is ingesteld, beschermt ze belangrijke mappen met eigen data tegen gijzelsoftware , ook wel Ransomware genoemd. Het wijzigen en verwijderen van de inhoud in die mappen wordt beperkt tot vooraf gedefinieerde programma's en processen. Welke mappen en programma's dat betreft is zelf in te stellen.

2. **Exploit protection**[5]
   Deze functie beschermt Windows tegen specifieke aanvalstechnieken die gericht zijn op het misbruiken van beveiligingslekken. Vroeger moest je die instellen met de apart te installeren tool EMET. Nu is het een standaard ingeschakeld onderdeel van Windows Defender. De standaardinstellingen zijn voor de meeste gebruikers afdoende.

3. **Attack Surface Reduction**[6]
   Met ASR wordt het risico van aanvallen op de beveiliging beperkt. Het is een vorm van beoordeling van het gedrag van programma's volgens zeven regels. Is een programma verdacht, dan wordt het geblokkeerd. ASR is een effectieve beveiliging tegen bijvoorbeeld Crypto-miners. Tevens is dit een belangrijke beveiliging tegen het uitvoeren van programmacode vanuit mailprogramma's. Het blokkeert naast .exe-bestanden ook scripts zoals .vbs en javascript. Komen deze bestanden vanaf een andere bron, dan zijn ze gewoon uitvoerbaar.
   ASR is niet standaard actief en niet via de interface van Defender te activeren. Wens je het in te schakelen dan kan dat alleen via lokaal Groepsbeleid (GPedit.msc) of met behulp van de PowerShell. Er zijn zeven verschillende regels die je kunt instellen. In de documentatie6 staat beschreven welke dat zijn. Mocht je het uitvoeren van code vanuit e-mailbijlagen willen blokkeren, dan voer je het volgende PowerShell-commando uit:

   ```
   Set-MpPreference -AttackSurfaceReductionRules_Ids
   BE9BA2D9 53EA 4CDC 84E5 9B1EEEE46550
   -AttackSurfaceReductionRules_Actions Enabled
   ```

   Voor de andere zes regels of het gebruik van Groepsbeleid, raadpleeg je de documentatie.[6]
   Wil je meer dan één regel aanpassen, zet dan de GUID's (de nummerreeks) en het schakelcommando (Enable, Disable, Auditmode), door komma's gescheiden in hetzelfde commando.
   Het is wijs om voorafgaande aan een wijziging te kijken hoe ASR staat ingesteld, dat kan met het PowerShell-commando:

   ```
   Get-MpPreference
   ```

   Controleer met dit commando na afloop ook of het gewenste effect bereikt is. Het commando:

   ```
   Set-MpPreference -AttackSurfaceReductionRules_Ids
   <rule ID 1>,<rule ID 2>,<rule ID 3>,<rule ID 4>
   -AttackSurfaceReductionRules_Actions Enabled,
   Enabled, Disabled, AuditMode
   ```

   zet de eerste twee regels aan, de derde wordt uitgezet en de vierde wordt in monitormodus geplaatst.

4. **Netwerkbeveiliging**[7]
   Netwerkbeveiliging is een Windows-driver die onderdeel van de kernel uitmaakt en al het uitgaande verkeer beveiligd. De beveiliging werkt analoog aan de safe-browsing beveiliging in een aantal browsers. Deze tool werkt dieper

in het systeem en voor al het internetverkeer. Deze tool voorkomt, op basis van een zwarte lijst in de Microsoft-cloud, dat programma's contact opnemen met gevaarlijke hosts. Informatie over inschakelen en configureren.[7] Met de PowerShell schakel je het met het volgende commando in:

```
Set-MpPreference -EnableNetworkProtection Enabled
```

Ook hier heb je de schakelopties: Enabled, Disabled en Auditmode.
Wil je de effecten van de instellingen testen dan is daar een website[8] voor. Deze beveiliging is overigens volledig afhankelijk van de lijsten die door Microsoft worden onderhouden.

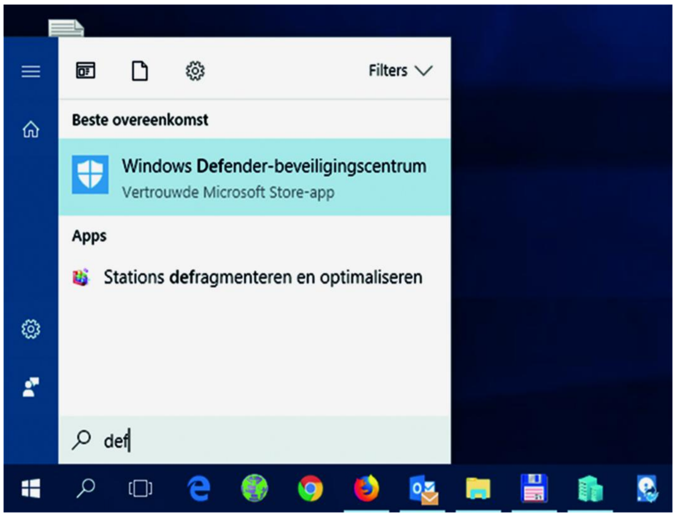
2 Beschermde mappen

De bediening van beschermde mappen zit diep verstopt in de Windows Defender interface. Deze geeft een extra laag van bescherming wanneer programma's wijzigingen trachten aan te brengen in je persoonlijke gegevens zoals Documenten, Afbeeldingen, je Bureaublad en alle andere mappen die je wenst te beschermen. In beginsel kan elk programma of ander proces alles aanpassen in die mappen. Wanneer je Controlled folder access inschakelt mogen alleen programma's die een Microsoft goed-stempel hebben wijzigingen in deze mappen aanbrengen. Daarnaast kun je zelf programma's aanmerken als veilig. Ongewenste software, waaronder Ransomware, wordt het zo onmogelijk gemaakt om ongewenste veranderingen aan te brengen.

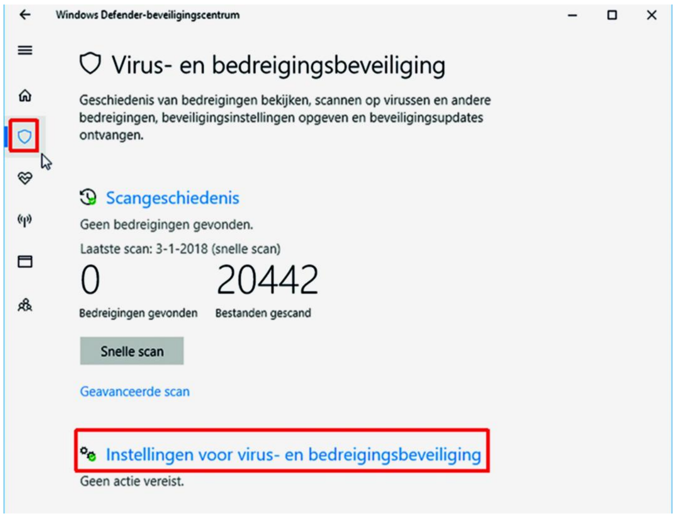
Controlled folder access beschermt je dus niet tegen het ongewenst inzien en kopiëren van je bestanden. Wanneer er Malware op je systeem actief is, kan het je bestanden wel downloaden en elders opslaan; het is alleen niet in staat om bestanden te wijzigen of te verwijderen.

2.1 Hoe zet je het aan?

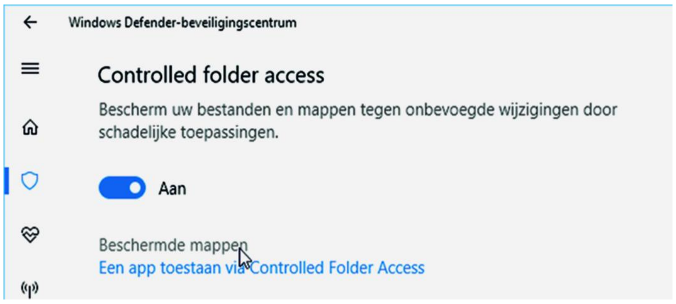
Hiertoe open je het Windows Defender-beveiligingscentrum door op de Windowstoets te drukken/klikken > Tik dan: '**def**' (Dus <**Win**+'**def**'>) en start het Windows Defender-beveiligingscentrum.



Klik op het **schildvormige icoon** (Virus- en bedreigingsbeveiliging) in de zijbalk van Windows Defender-beveiligingscentrum > klik op '**Instellingen voor virus- en bedreigingsbeveiliging**'



Blader nu naar beneden en zet het schuifje bij '**Controlled folder access**' op aan. Geef toestemming op de vraag van Gebruikersaccountbeheer. Mocht je deze optie niet zien, dan heb je de upgrade naar versie 1709 nog niet. Het is een omslachtige manier om er te komen. Helaas heb ik nog geen snellere manier kunnen vinden.



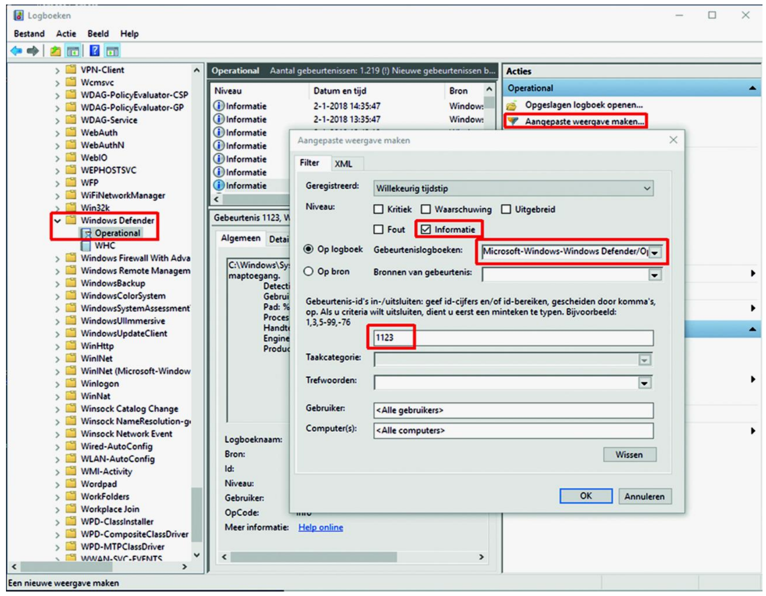
Na het aanzetten van Controlled folder access kun je klikken op '**Beschermde mappen**' om de mappen te selecteren die je wenst te beschermen.
Standaard worden de Windows-systeemmappen, de openbare mappen en gebruikersmappen beschermd. Dat zijn Documenten, Afbeeldingen, Muziek, Video's, Bureaublad en Favorieten onder de gebruikersmap. Dit zijn vaste mappen die je niet kunt verwijderen. Mocht je net als ik ook waardevolle data op een andere plek willen beschermen, dan kun je dat doen, door op de knop [+] 'Een beveiligde map toevoegen' te klikken. Zo beveilig je alle waardevolle bestanden, in door jezelf aangemaakte mappen, tegen gijzeling. en dan die map(pen) toevoegen.

2.2 Een programma toegang geven tot je bestanden

Windows probeert op een slimme wijze te achterhalen welke programma's schrijftoegang mogen krijgen tot deze mappen. Windows Defender kent een groot aantal veilige programma's en geeft deze de benodigde rechten. Dat selectieproces is niet volledig helder. Denkelijk wordt het bepaald op basis van door Microsoft gesigneerde bestanden en veilige apps uit de Store. Dat vermindert het geklooi om de juiste programma's toegang te geven. Dat zijn er sowieso al genoeg. Niet alle programma's die je zou verwachten worden toegestaan.

Wanneer je een programma toestaat, geef je het toegang tot alle beschermde mappen. Helaas kun je dat niet verder beperken tot alleen gespecificeerde mappen.
Mocht een programma wat willen wijzigen in een beschermde map, dan wordt er een Virus- en bedreigingsbeveiligingsbericht: *'Niet-toegestane wijziging geblokkeerd'* getoond in het Notificatiecentrum. De melding geeft aan welk programma in welke map iets trachtte te wijzigen.
Wanneer je deze melding ziet, en het betreft een programma dat je veilig acht, kun je dat aan de lijst van veilige programma's toevoegen. Twijfel je over de veiligheid van een programma, scan het dan eerst op de site: virustotal.com.
De snelste wijze om op de plek te komen waar je dat kunt doen, is klikken op de melding. Dan wordt je gebracht naar de plek waar het programma toegevoegd kan worden. Dat is het Windows Defender-beveiligingscentrum > Klik op het pictogram met het **schild** > klik op **'Instellingen voor virus- en bedreigingsbeveiliging'** > Blader naar **'Een app toestaan via Controlled Folder Access'**.

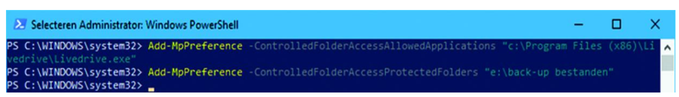
Klik nu op [+] 'Een toegestane app toevoegen'
Blader nu naar de locatie waar het desbetreffende programma staat. Je zult het uitvoerbare bestand - meestal een .exe - dienen te vinden dat bij de applicatie hoort. Ken je de juiste locatie niet, dan is het vaak te vinden door een **Rechtsklik** (Staat het programma op de taakbalk dan **Shift+Rechtsklik**) op de snelkoppeling behorende bij het programma > **Eigenschappen**. Het bewuste .exe bestand staat op het **tabblad**: **Snelkoppeling** in het veld: **Doel**. Selecteer de inhoud van Doel, kopieer het met <Ctrl+C> en plak het dan <Ctrl+V> in het veld **Bestandsnaam** van het Verkennervenster dat zich opende toen je op de [+] drukte in Windows Defender-beveiligingscentrum.
Mocht je de melding even hebben gemist, besef dan dat die nog in het Notificatiecentrum staat, totdat je ook daar de melding hebt gewist. Overigens wordt er ook een gebeurtenis in het logboek geschreven.
Die kun je inzien door de logboeken te openen > **Logboeken Toepassingen en Services** > **Microsoft** > **Windows** > **Windows Defender** > **Operational**. Je kunt dan ook een aangepaste weergave voor dat logboek, met die weergave maken. Selecteer het bewuste logboek en klik dan in de rechterbalk onder Acties op **Aangepaste weergave maken** en vul het in zoals in de afbeelding. Het betreft een gebeurtenis van het niveau Informatie met ID: 1123.



Nadat je op **[OK]** hebt gedrukt, wordt een venster geopend waarin je de weergave een naam kunt geven. Bijvoorbeeld: Geweigerde toegang beveiligde mappen. Je vindt deze weergave, tenzij je anders hebt aangegeven, onder het kopje: 'Aangepaste weergaven'.
Ben je al dat geklik voor het toevoegen van een beveiligde map en een toegestane app beu, dan kun je sneller resultaat bereiken via een Power Shell-commando uitgevoerd als Admin. Daarvoor zijn de volgende twee commando's beschikbaar:

Programma of proces toevoegen:
```
Add-MpPreference -ControlledFolderAccessAllowed-
Applications "<Programma inclusief het pad>"
```

Beschermde map toevoegen:
```
Add-MpPreference -ControlledFolderAccessProtected-
Folders "<De map die je wenst te beschermen>"
```



Dit is met name handig wanneer je net Controlled folder access hebt geactiveerd en uiteraard voor systeembeheerders om zo de instellingen eenvoudig over meerdere machines uit te rollen.

TiP: Zorg ervoor dat de browsercaches van de diverse browsers zich niet in beschermd gebied bevinden. Wanneer dat wel zo is, worden de browsers in belangrijke mate vertraagd. Wil je weten hoe je de caches van verschillende browsers verplaatst? Lees dan hier.[9]

3 Exploit protection

Ook de Exploit protection zit diep weg in de Windows Defender-beveiligingscentrum interface. Die is standaard zo geconfigureerd dat die voor de meeste mensen afdoende is. Heb je geen zin om je erin te verdiepen of zie je de noodzaak niet, laat het dan zoals het is en sla dit hoofdstuk met een gerust hart over.

Exploit protection gebruikt ondoorzichtige termen, zoals Controlestroombeveiliging (CFG), Preventie van gegevensuitvoering (DEP) en nog een aantal. Standaard staan al deze in-

stellingen aan. Wil je precies weten wat ze betekenen? Lees dan de Engelstalige uitleg.[5] In het kort komt het erop neer dat de beveiliging kijkt naar de code en het gedrag van een programma. Bevat de code bekende aanvalstechnieken of is het gedrag verdacht doordat het acties tracht uit te voeren in gebieden van het geheugen en het operatingsysteem, dan wordt de uitvoering ervan geblokkeerd.
Het kan voorkomen dat deze bescherming compatibiliteitsproblemen veroorzaakt. Wellicht moet je voor een bepaald programma dat voor jou onmisbaar is een uitzondering toevoegen. Gelukkig heeft Microsoft al diverse bekende programma's aan de uitzonderingslijst toegevoegd.

3.1 Hoe controleer je het?

Je kunt Exploit Protection vinden in het Windows Defender-beveiligingscentrum <**Win**+'**def**'>. Klik op het **venster-icoon** (App- en browserbeheer) in de zijbalk van het Windows Defender-beveiligingscentrum >

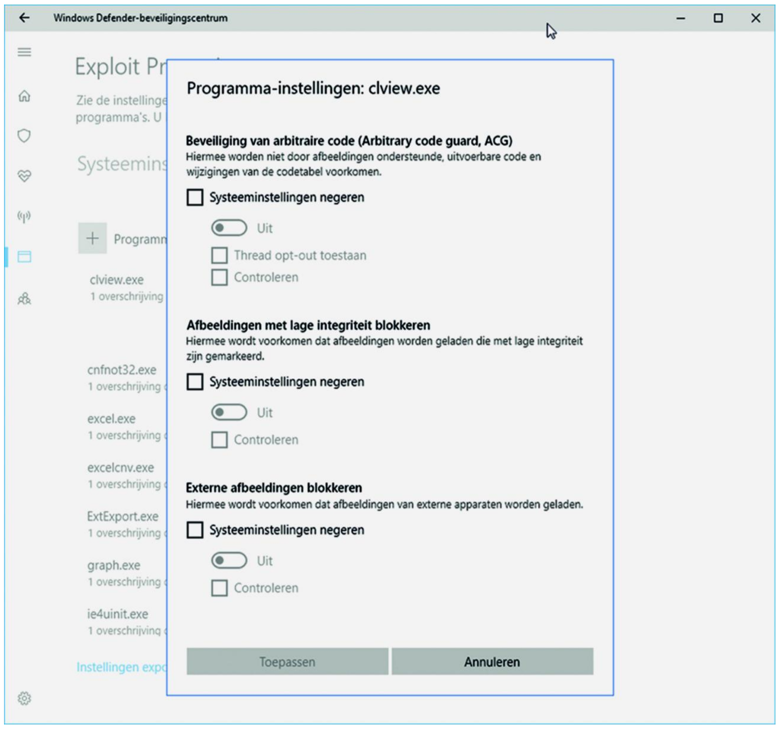
Blader naar beneden totdat **Exploit Protection** verschijnt > Klik nu op '**Instellingen voor Exploit Protection**'. Nu kun je Exploit Protection controleren en desgewenst aanpassen.

3.2 Welke instellingen?

Wellicht wil je deze instellingen nooit wijzigen, maar het kán wel. Weet wat je doet en raadpleeg de handleiding![5] Noteer de oorspronkelijke instellingen en wijzigingen, of maak er schermafdrukken van!
Je ziet hieronder twee instellingscategorieën: Systeeminstellingen en de meer uitgebreide Programma-instellingen.

Onder Systeeminstellingen staan diverse opties met een summiere uitleg. Uitgezonderd ASLR staat alles ingeschakeld. ASLR staat en stond systeemwijd al ingeschakeld voor programma's die met een speciale compiler-optie gemaakt zijn. Het inschakelen van ASLR voor alle programma's kan tot ongewenste effecten leiden. Pas daarmee op!

Onder Programma-instellingen zie je een lijst van diverse programma's met hun instellingen. De opties die je ziet zijn de algemene systeeminstellingen die je zou kunnen aanpassen. Pas vooral op met systeemprocessen. Deze staan hier om een reden. Je wilt immers een werkbaar systeem! Rommel daarom niet zomaar met de instellingen.



Het is mogelijk om eigen regels voor specifieke programma's te maken. Doe dat alleen als er noodzaak toe is. Wanneer je het pad niet specificeert bij een programma, dan geldt de regel voor alle programma's met die naam, onafhankelijk van map waarin het zich bevindt. Maak je een eigen regel, specificeer dan ook het exacte pad om niet per ongeluk een programma met dezelfde naam vrij te geven of te beknotten. Meer informatie vind je ook hier weer in de handleiding.[5]

4 Tot slot

Microsoft heeft een grote stap vooruit gemaakt in de beveiliging van Windows. De interface van het Windows Defender-beveiligingscentrum is helaas nogal omslachtig en niet intuïtief. Ook ontbreken daar de instellingen voor Attack Surface Reduction en voor Netwerkbeveiliging, al was het alleen maar om de optie aan of uit te zetten.

Bedenk ook dat absolute veiligheid niet bestaat. Het beveiligen van je gegevens blijft een ratrace tussen de makers van malware en de beveiligingsbedrijven. Daarom is er naar mijn idee maar één manier om jezelf tegen ongewenste indringers te beschermen en dat is, naast het regelmatig updaten van Windows en de programma's: Back-up, Back-up en Back-up! De hierboven beschreven beveiliging is dan ook nooit een vervanger van een goede back-up.[10]

Links:

Verkorte links kunnen je zo maar naar een onveilige site verwijzen. Wees dus voorzichtig!
Testen kun je met: www.urlunshortener.com of www.unshorten.it

1 Back-uppen moet	http://bit.ly/r-bum
2 Defender-beveiligingscentrum	http://bit.ly/r-def
3 Antivirustest	http://bit.ly/r-avtest
4 Controlled Folder Access	http://bit.ly/r-cfa
5 Exploit Protection	http://bit.ly/r-ep
6 Attack Surface Reduction	http://bit.ly/r-asr
7 Netwerkbeveiliging	http://bit.ly/r-nb
8 SmartScreentests	http://bit.ly/r-sct
9 Browsercache verplaatsen	http://bit.ly/r-bc
10 Gratis back-up	http://bit.ly/r-dbus
Dit artikel	http://reindejong.nl/veilig10
Mijn eigen site	http://reindejong.nl