Auteurs: Vincent van Dijk en Chris de Vries. Vincent van Dijk is eigenaar van Security Scientist en is bereikbaar via vincent@securityscientist.net. Chris de Vries is redacteur van het IB Magazine en daarnaast eigenaar van De Vries *Impuls* Management, hij is bereikbaar via impuls@euronet.nl.

Hoe beveilig je een Windows laptop of computer?

HULPGIDS BEVEILIGING VOOR HET KLEINBEDRIJF (DEEL 3)

In de vorige uitgave vroeg Chris naar gereedschappen welke het mkb kan gebruiken om een bedrijf te beveiligen. Firewalls, password managers en antivirus zijn erg breed in te zetten en helpen je om vanuit een holistisch oogpunt een keuze te maken.

Toch is het goed om in te zoomen op specifieke systemen en applicaties die we dagelijks gebruiken: je laptop, e-mail of online software. Dit artikel zal wat dieper inzoomen op Windows laptops en PC's die je dagelijks gebruikt om je werk te verrichten.

Vincent, ik heb een Windows laptop, mijn collega's gebruiken ook Windows. Waar moet ik naar kijken als ik een Windows laptop wil beveiligen?

Bij een Windows laptop gaat het er niet alleen om dat je de juiste beveiligingstools hebt geïnstalleerd. Net zoals thuis, kun je niet alleen volstaan met het installeren van een goed slot en het ophangen van een camera. Je moet er ook voor zorgen dat kostbare spullen niet zomaar in het zicht staan en je moet altijd de deur op slot doen wanneer je weggaat.
Om jouw digitale Windows-huis te beveiligen, kijken we naar drie categorieën:

1. Hygiëne
2. Veilige configuratie
3. Systeem kennis

1. Hygiëne

Bij hygiëne gaat het erom dat je laptop mooi schoon is. Na verloop van tijd verzamelen onze computers onnodige bestanden, tijdelijke gegevens en overbodige programma's die kostbare opslagruimte in beslag nemen en prestaties vertragen. Rommel die ook je dreigingslandschap vergroten.

Zorg ervoor dat je die rommel verwijdert. Ga regelmatig door je geïnstalleerde applicaties heen en verwijder alle applicaties die je niet meer nodig hebt of nooit meer gebruikt. Gebruik ook regelmatig de ingebouwde tool Schijfopruiming om tijdelijke bestanden, systeemcaches en andere onnodige gegevens te verwijderen.

Door het vele gebruik van browsers creëer je tegenwoordig ook een hoop rommel in de browser. Webbrowsers verzamelen tijdelijke bestanden, cookies en browsegeschiedenis, die de prestaties kunnen beïnvloeden en de privacy in gevaar kunnen brengen. Maak regelmatig de cache van je browser leeg en verwijder cookies alsook de browsegeschiedenis om je browse-ervaring fris en veilig te houden. Verken de instellingen van jouw browser om extensies te beheren en verwijder onnodige of verouderde 'Add-ons'. Ik raad aan om twee belangrijke 'Add-ons' te installeren in je browser:

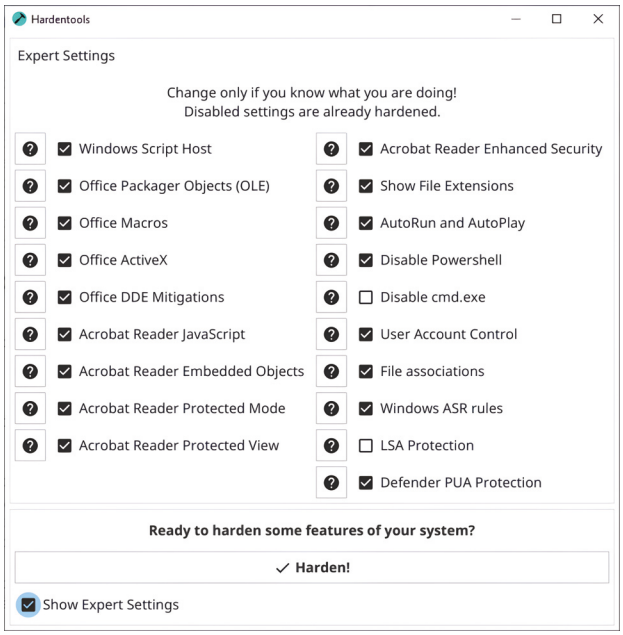
1. 'Adblocker' voor het blokkeren van virussen, die via advertenties verspreid worden. Gebruik *UBlock Origin* en vermijd de andere AdBlockers. Ook AdBlockers hebben een reputatie om virussen te bevatten (1).
2. 'Cookie Auto delete' zorgt ervoor dat de cookies van je webbrowsers mooi opgeruimd blijven (2).

Naast het opruimen van onnodige applicaties is het ook essentieel om een password manager te gebruiken en sterke wachtwoorden te hanteren. Een password manager helpt je bij het veilig beheren van al je wachtwoorden, waardoor je niet telkens hetzelfde wachtwoord gebruikt en je sterkere wachtwoorden kunt genereren en onthouden. Zie ook IB Magazine 2- 2023, de artikelen van Lex Borger en Menno Vermeulen over dit onderwerp.
Ook is het verstandig om regelmatig Windows opnieuw te installeren, bij voorkeur minimaal jaarlijks, maar vaker mag. Door Windows opnieuw te installeren worden eventuele ongewenste programma's, virussen of andere vormen van malware verwijderd, waardoor jouw laptop schoon en efficiënt blijft werken. Het helpt ook om de prestaties van je systeem te verbeteren en eventuele softwareproblemen op te lossen.

2. Veilige configuratie

Over het algemeen heb je geen duur antivirusprogramma nodig om een veilige Windows laptop te hebben - Windows komt al met een prima antivirusprogramma: Windows Defender en Firewall. Let op: controleer of deze tools aanstaan, met name door het gebruik van andere programma's kan Defender automatisch uitgezet worden. Bovenop de standaard configuratie is het verstandig om het systeem te voorzien van een paar veilige instellingen. Dat gaat het makkelijkst door HardenTools (3) te downloaden en te activeren. Deze tool zal ervoor zorgen dat standaard alle risico-

volle functies, zoals: Powershell en MS Office macro's uitgeschakeld worden.



Figuur 1: HardenTools zet tal van risicovolle applicaties uit.

Om de veiligheid van je Windows systeem nog meer te verhogen is het goed om een administratoraccount te gebruiken. Door een apart administratoraccount te hebben, creëer je een onderscheid tussen dagelijkse taken en administratieve functies die verhoogde privileges vereisen.

Je kunt een apart administratoraccount maken met de volgende stappen in Windows 11 (4)

1. Inschakeling van het administratoraccount: ga naar de instellingen van Computerbeheer, ga naar Gebruikers en schakel het administratoraccount in, dat standaard is uitgeschakeld. Stel een sterk wachtwoord in voor dit account.
2. Wijziging gebruikerstype: open het Configuratiescherm, ga naar Gebruikersaccounts en klik op het gebruikersaccount dat moet worden gewijzigd. Schakel het accounttype om van administrator naar standaardgebruiker.
3. Instelling gebruikersaccountbeheer op de hoogste stand: open de instellingen voor Gebruikersaccountbeheer en selecteer de optie welke altijd melding geeft wanneer toepassingen proberen software te installeren of wijzigingen aan te brengen in de computer- of Windowsinstellingen. Bevestig de wijziging.
4. Test de nieuwe instellingen: download een softwareprogramma van internet en probeer het te installeren. Het systeem vraagt nu eerst om toestemming van het administratoraccount voordat de installatie wordt toegestaan.

Additioneel zijn er meerdere security features die je kunt aanzetten in Windows 10/11. Hier zijn nog vijf features waar je naar kunt kijken. Let wel op, voor sommige features heb je een Windows pro licentie nodig (5).

1. Windows Sandbox (6)
Windows Sandbox is een geïsoleerde virtuele omgeving waarin je verdachte programma's kunt uitvoeren zonder risico voor het hoofdsysteem. Het biedt een tijdelijke omgeving waarin je bestanden kunt kopiëren, programma's kunt testen en vervolgens de Sandbox kunt sluiten, waarbij alle wijzigingen worden verwijderd.

2. Application Guard (7)
Application Guard creëert een geïsoleerd browservenster, vooral in Microsoft Edge, waarin je potentieel schadelijke websites veilig kunt openen. Het voorkomt dat kwaadwillende inhoud of malware zich verspreidt naar het hoofdsysteem door een gescheiden en beveiligde omgeving te bieden voor het openen van webpagina's.

3. Reputation-based protection (8)
Reputation-based protection omvat functies zoals *SmartScreen* en phishing-bescherming. *SmartScreen* beoordeelt de betrouwbaarheid van gedownloade bestanden en waarschuwt je als een bestand een slechte reputatie heeft. Phishing-bescherming waarschuwt je voor potentieel scha-

delijke of frauduleuze websites die proberen persoonlijke gegevens te stelen.

4. Device protection (9)
Windows biedt ingebouwde functies zoals core-isolatie en geheugenintegriteit om jouw apparaat te beschermen tegen kwaadaardige software-aanvallen. De beveiligingsprocessor biedt extra versleuteling en de functie *Secure boot* voorkomt dat malware, zoals rootkits, worden geladen wanneer het apparaat start.

5. Controlled folder access (10)
Controlled folder access is een functie die beperkingen oplegt aan welke programma's toegang hebben tot bepaalde mappen op je systeem. Het beschermt tegen ransomware-aanvallen door te voorkomen dat ongeautoriseerde programma's belangrijke mappen wijzigen.
Onderaan het artikel hebben wij een aantal links opgenomen. Via deze links kun je deze security features van Windows zelf bekijken en aanpassen.

3. Systeem kennis

Een systeem is nooit statisch, het is geen steen. Jouw Windows laptop verandert continu, als gevolg van updates, nieuwe applicaties en door gebruik. Om een veilig huis te bouwen en te onderhouden moet je kennis hebben van gereedschap, je hoeft geen expert te zijn, maar je moet wel weten dat je een hamer niet gebruikt om een schroef in de muur te slaan. Zo moet je ook kennis en kunde hebben van jouw Windows systeem om verdacht gedrag te kunnen zien of om een laptop goed te onderhouden.

Een belangrijk component voor jouw systeemkennis zijn de Windows logs. Het bestuderen van de Windows logs zorgt ervoor dat je beter grip krijgt op wat er allemaal precies gebeurt in jouw Windows systeem. Om de Windows logboeken te bekijken en te filteren, volg je de onderstaande stappen:

1. Open het menu Start en typ *'Event Viewer'* in het zoekvak. Klik op *'Event Viewer'* in de zoekresultaten om het venster *'Event Viewer'* te openen.
2. In het linkerdeelvenster van *'Event Viewer'* zie je verschillende logboekcategorieën, zoals o.a. Toepassing-, Beveiliging- en Systeemlogboeken. Klik op de gewenste categorie om de bijbehorende logboeken uit te vouwen.
3. Selecteer het specifieke logboek waarin je geïnteresseerd bent, bijvoorbeeld *'Beveiligingslogboeken'*. De gebeurtenissen in dat logboek worden weergegeven in het rechterdeelvenster.
4. Om gebeurtenissen te filteren, klik je met de rechtermuisknop op het gewenste logboek en selecteer je *'Filter Current Log'* of *'Filteren op huidig logboek'*. Hierdoor wordt het venster *'Filter Current Log'* geopend.
5. In het venster *'Filter Current Log'* kun je verschillende filtercriteria instellen, zoals logboekbron, Event-ID, trefwoorden, datum/tijd, enzovoort. Pas de filters aan op basis van jouw specifieke vereisten en klik op *'OK'*.
6. Na het toepassen van de filters worden alleen de logs weergegeven die aan de opgegeven criteria voldoen.

Op deze manier kun je de Windows logboeken bekijken en filteren om specifieke gebeurtenissen te vinden en relevante informatie te verkrijgen. Houd er rekening mee dat het gebruik van de Event Viewer mogelijk beheerdersrechten vereist.

De basis van alle logs zijn de zogeheten EventIDs. Deze identificatie nummers geven aan waar een log over gaat. Als je wilt zoeken naar logs kun je het beste zoeken naar verdachte EventIDs. De website *Ultimate Windows Security* heeft de beste beschrijvingen van alle Windows EventIDs met uitleg bij elke log (11).

In een Windows systeem zijn er verschillende logs waar je op moet letten om de beveiliging te waarborgen en potentiële bedreigingen te monitoren. Hier zijn de belangrijkste gebeurtenissen die genoemd worden in de tekst (12):

1. Event -ID 4688: deze gebeurtenis geeft aan wanneer er wordt ingelogd op een systeem en verstrekt informatie over het type gebruiker dat heeft ingelogd.

Let erop dat je nooit vertrouwelijke informatie vermeldt in de gestelde vragen, dat is stap 1 voor een veilige ICT-omgeving!

2. Event -ID 1102: deze gebeurtenis duidt op het wissen van een logboek, wat ongebruikelijk is in een normale omgeving en kan wijzen op pogingen van aanvallers om sporen te verbergen.
3. Event -ID 4670: deze gebeurtenis geeft wijzigingen weer in objectmachtigingen die gemonitord moeten worden, vooral in combinatie met het inschakelen van controlebeleid met betrekking tot machtigingen voor schrijven, DAC-wijzigingen of eigendomsoverdracht.
4. Event -ID 4624: deze gebeurtenis vertegenwoordigt een succesvolle accountlogin en wordt beschouwd als een basisgebeurtenis bij inloggen door de bevoegde gebruiker, welke regelmatig in de omgeving moet voorkomen.
5. Event -ID 4672: wanneer deze log gecombineerd wordt met Event -ID 4624, duidt dit op het toewijzen van speciale rechten aan een nieuwe login, wat kan wijzen op potentiële aanvallen zoals '*pash the hash*' (een hacking techniek!). Het is raadzaam om extra aandacht te besteden aan deze combinatie.
6. Event -ID 10 (met Sysmon geïnstalleerd): deze gebeurtenis is specifiek voor Sysmon, een tool die de analyse verbetert, en toegang geeft tot het LSASS-proces (Local Security Authority Subsystem Service), wat relevant kan zijn voor het detecteren van tools die gebruikt worden in '*pash the hash*'-aanvallen.
7. Event-ID 1116 (in Windows Defender): deze gebeurtenis, te vinden in de logboeken van Windows Defender-antivirus, geeft aan dat er malware of mogelijk onveilige software is gedetecteerd of geïnstalleerd op het systeem.

Wij kunnen ons voorstellen dat bovenstaande niet één-twee-drie door jullie, mkb-lezers, is toe te passen of dat er vragen opkomen. Gebruik dan ook de mogelijkheid om via LinkedIn vragen te stellen aan ons. Wij komen er dan zeker op terug. Via LinkedIn, via een directe reactie (zeker wanneer het om vertrouwelijke informatie gaat) en anders via IB Magazine. Let erop dat je nooit vertrouwelijke informatie vermeldt in de gestelde vragen, dat is stap 1 voor een veilige ICT-omgeving!

Referenties

(1) https://ublockorigin.com/
(2) https://duckduckgo.com/?t=ffab&q=coockie+auto+delete&ia=web
(3) https://github.com/securitywithoutborders/hardentools
(4) https://www.youtube.com/watch?v=TOpups3RDYA
(5) https://www.youtube.com/watch?v=uljX4aOoeaQ
(6) https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-sandbox/windows-sandbox-overview
(7) https://learn.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-application-guard/md-app-guard-overview
(8) https://support.microsoft.com/en-us/windows/protect-your-pc-from-potentially-unwanted-applications-c7668a25-174e-3b78-0191-faf0607f7a6e
(9) https://support.microsoft.com/en-us/windows/device-protection-in-windows-security-afa11526-de57-b1c5-599f-3a4c6a61c5e2
(10) https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-controlled-folders?view=o365-worldwide
(11) https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/-default.aspx
(12) https://www.csoonline.com/article/3561889/the-most-important-windows-10-security-event-log-ids-to-monitor.html