TiPisch Rhino – Browserbeveiliging

Rein de Jong

Beveilig je browser tegen indringers!

Ook last van ongewenste gasten in je browser? Ervaar jij – of je omgeving – dat je browser is gekaapt of besmet? Zie je een werkbalk (toolbar) die je niet bewust hebt geïnstalleerd? Dan is er sprake van zogenaamde 'Potentially Unwanted Programs', kortweg PUP's. Deze PUP's behoren niet tot de traditionele malware. Antivirusprogramma's vinden het maar moeilijke zaken omdat ze niet altijd ongewenst zijn. Ik snap het niet, maar er bestaan mensen die een aantal van deze PUP's handig vinden. Denk hierbij aan de toolbars van Ask, eBay en FoxyTunes. Ik hoef ze niet! Echt schadelijk zijn de PUP's niet. Vaak alleen maar vervelend omdat ze kostbare (beeldscherm)ruimte innemen.

Naast PUP's zijn browsers ook een ingang die door cybercriminelen wordt gebruikt om malware je computer binnen te loodsen. Doordat Microsoft veel mechanismen heeft toegevoegd aan Windows 8.1 wordt het steeds lastiger om gebruik te maken van de gaten in het operating-systeem. Daarom zullen de criminelen proberen toegang tot je computer te krijgen. Daarbij maken ze meestal gebruik van de browser en e-mail. Dat wordt social engineering[1] genoemd.

Gedragsregels

Alles staat of valt met hoe je zelf met internet omgaat. Ter voorkoming van PUP's en om het besmettingsgevaar te verkleinen, is een aantal gedragsregels aan te bevelen:
Download software alleen van de bron, bij voorkeur van de site van de maker. Dus niet van download-portals zoals xxx.download.com, die meestal bovenaan staan in de lijst van de zoekmachines. Ik hanteer meestal de regel dat pas vanaf de zevende link de kans op een goed resultaat het grootst is.
Populaire gratis programma's worden vaak in een pakketje samengevoegd met ongewenste programma's. Dat installatiepakket wordt dan aangeboden op onofficiële sites. Dat is het aas dat je wordt voorgehouden. Download je dat aas, dan komt er met het gewenste programma veel ongewenste zooi mee. Let dus goed op bij het installeren van gratis programma's. Welke opties worden geboden (vaak staan ze al standaard aangevinkt) en kijk goed of je die al dan niet wenst. Vaak zijn de opties alleen te zien wanneer je de uitgebreide (user-defined of enhanced) installatiemethode kiest. Kies die dan ook ALTIJD!
Soms is de 'Overslaan'-knop grijs gemaakt zodat de indruk wordt gewekt dat die niet aanklikbaar is. Probeer het toch! Ook worden er wel dubbele ontkenningen gebruikt om je te misleiden.
Update Windows en andere belangrijke software regelmatig. Denk vooral aan veelgebruikte programma's als Java, Flash, Silverlight, PDF-reader en natuurlijk je virusscanner. Nog beter is het om Flash in het geheel niet te gebruiken. De meeste sites schakelen dan zelf om naar het veiliger HTML5.
Gebruik zuivere zoekmachines, zoals Startpage.com en/of Duckduckgo.com. Met 'zuiver' bedoel ik zoekmachines zonder winstoogmerk. Google en Bing zijn geen zuivere zoekmachines omdat ze gesponsorde links bovenaan in de resultaten plaatsen.
Vermijd het gebruik van Javascript in de browser (NoScript-plug-in gebruiken of via de instellingen van je browser Javascript verbieden).
Let op: Javascript is compleet wat anders dan Java!
Denk na voordat je een werkbalk installeert. Heb je die écht nodig?
En last but not least: installeer alleen datgene waar je behoefte aan hebt. Niet omdat een ander beweert dat je er behoefte aan zou moeten hebben!

Plug-ins

Plug-ins en extensies (toevoegingen) zijn kleine programma's die de functionaliteit van de browser uitbreiden. Dit kan ten goede of ten kwade worden gebruikt. Ten goede om je browser veiliger te maken en ongewenste reclame en statistiekprogramma's te weren, zoals Google Analytics. Ten kwade vanwege het feit dat er ogenschijnlijk nuttige extensies zijn die echter spyware bevatten, zoals WOT (Web of Trust) en Adblock.

Voorbeelden van erg nuttige plug-ins zijn:

HitManPro Alert[2] (alle browsers).
Dit is eigenlijk geen plug-in, maar een programma dat start voordat de browser start. Het is een gratis programma dat de integriteit van de browser test en gebruikers waarschuwt wanneer veilig winkelen en bankieren niet meer gegarandeerd is. Ook beschermt HMP Alert tegen malware die je data versleutelt (Cryptolockers).

Adblock Plus[3] (Internet Explorer, Chrome, Firefox, Safari, Opera).
Deze uitbreiding van de browser blokkeert reclameuitingen op websites. Ook worden de reclames van Facebook en YouTube geblokkeerd. Je kunt aangeven wat wel en wat niet wordt geblokkeerd. Ik verkies Adblock Plus (ABP) boven Adblock omdat Adblock geen open ontwikkeling meer kent en dus niet gecontroleerd kan worden. Bovendien 'volgt' Adblock zijn gebruikers en is dus spyware. ABP is open en transparant; de gebruikers blijven anoniem. ABP laat sommige advertenties door, mits deze voldoen aan de regels van acceptabele advertenties[4].

NoScript[5] (Firefox)
Volgens het antivirusbedrijf Malwarebytes is de Firefox-uitbreiding NoScript misschien wel de beste methode om je browser te beveiligen. De extensie verijdelt het gebruik van actieve inhoud op websites, zoals JavaScript, malware plug-ins en volgprogramma's (trackers). Bovendien biedt het bescherming tegen XSS (scripts gestart door andere websites). Door de beveiliging van NoScript kan het zijn dat websites die zwaar leunen op Javascript, niet meer helemaal goed getoond wor-den. Als gebruiker

moet je zelf kiezen welke scripts uitgevoerd mogen worden en welke niet. Het gebruik van NoScript vereist kennis en discipline van de gebruiker. Je dient als gebruiker in te schatten welke site wel en welke niet toegestaan wordt. NoScript geeft je een goed beeld van de verwevenheid van het internet.
Kijk maar eens, met NoScript ingeschakeld, bij www.wehkamp.nl. Sites die bij mij standaard geblokkeerd staan zijn: Google Analytics en Google Ad Service. Aanvankelijk moet je vertrouwde sites even opbouwen en wennen aan de meldingen van NoScript. Doe je dat en heb je de nodige discipline, dan is de combinatie van Firefox en NoScript de veiligste om het internet te doorkruisen.
Wanneer een site niet goed toont zonder Javascript, zie ik dat steeds meer als een tekortkoming van die site. Het kan immers gemakkelijk anders en zonder gevaarlijke scripts. Mocht je de top-level site (dat is de website die je intikt of aanklikt via de zoekmachine) vertrouwen, dan zou je Javascript kunnen toestaan.

Eventueel zou je in de Opties 'Standaard Top-levelsites tijdelijk toestaan' aan kunnen vinken. En een vinkje zetten bij 'Via een bladwijzer geopende sites toestaan'. Dat maakt het wennen aan NoScript eenvoudiger. Later kun je die vinkjes weghalen, wanneer je meer vertrouwd bent met de NoScript plug-in.

ScriptSafe[6] (Chrome)
Helaas is NoScript er niet voor Chrome. Echter, wat NoScript is voor Firefox, is ScriptSafe in beperkte mate voor Google Chrome. Ook deze extensie blokkeert Javascript en kan sites op een witte danwel zwarte lijst plaatsen.

Ghostery[7] (Internet Explorer, Chrome, Firefox, Safari, Opera).
Net als Adblock Plus en NoScript blokkeert Ghostery trackers. Op het internet vind je hele discussies of Ghostery al dan niet overbodig is. Gebruik je ABP en/of NoScript, dan is het antwoord JA! Vaak wordt Ghostery naast ABP gebruikt en dan overlappen ze elkaars functionaliteit. Dat kan tot ongewenste resultaten leiden. Ghostery is in handen van een advertentiebedrijf en dat maakt het in mijn ogen verdacht. Ik verkies Adblock Plus boven Ghostery. Wil je toch ABP en Ghostery naast el-kaar gebruiken, stel Ghostery dan zo in dat het alleen de tracking cookies blokkeert.
Zelf gebruik ik HMP Alert in combinatie met Firefox waarin de plug-ins Adblock Plus en NoScript zijn aangebracht. Wil ik echter zo anoniem mogelijk surfen, bijv. voor gezondheidsvragen of het opzoeken van andere privacygevoelige materie, dan maak ik gebruik van TorBrowser. TorBrowser gebruikt het open anonieme Onion Netwerk (een ui bestaat uit meerdere lagen) dat gebruik maakt van gelaagde virtuele tunnels.

Wanneer het toch misgaat…

Het kan altijd gebeuren dat er, ondanks al je voorzorgsmaatregelen, toch iets doorslipt. Daarvoor wil ik twee programma's aanbevelen. Beide programma's kun je uitvoeren naast je huidige antivirusprogramma's en ze worden alleen op je eigen commando actief. Beide zijn second opinionscanners waarbij AdwCleaner zich vooral richt op malware en PUP's die via de browser binnenkomen. HitManPro presteert het beste in 'vuil water'.

AdwCleaner[8]
Dit gratis portable programma scant de computer op malware, toolbars, hijackers en andere PUP's. Het ondersteunt de browsers Internet Explorer, Chrome en Firefox. Je start de scan en kunt dan zelf bepalen wat er verwijderd wordt. Kijk vooral de tab 'Folders' (Mappen) goed na; bij mij wil AdwCleaner altijd, ten onrechte, de map C:\Util verwijderen. Mocht het programma onverhoopt te veel verwijderen, dan kan dat vanuit de quarantaine worden teruggeplaatst.

HitManPro[9]
HitManPro (HMP) is weer helemaal terug. HMP is nu een volwaardige malwarescanner die het vooral in een besmette omgeving erg goed doet. De resultaten die HMP haalt zijn boven-gemiddeld goed. Het is als second opinionscanner een prima aanvulling op je standaard antivirusprogramma.
Wanneer HMP malware detecteert, kan het deze gratis verwijderen nadat je recent de 30 dagen proeflicentie hebt geactiveerd. Mocht je daarna malware met HMP wensen te verwijderen, dan moet je betalen of de gedetecteerde malware handmatig verwijderen. HMP blijft na afloop van de 30 dagenlicentie nog altijd prima scannen. Het is verstandig om beide programma's minimaal één keer per maand uit te voeren. Je bestaande antivirus-programma is namelijk niet onfeilbaar. Bovenstaande programma's kun je beschouwen als een bewaker op ronde en een virusprogramma als de portier bij de ingang.

Tot slot

Ook met al deze maatregelen kan het nog steeds misgaan. De allerbeste beveiliging is: Back-up, back-up, back-up, back-up! Ik kan het niet genoeg benadrukken. Zorg ervoor dat je je back-up locatie, vanaf je standaard gebruikte account, uitsluitend via alleenlezen toegang kunt benaderen. Maak een apart back-up account dat jouw gegevens kan lezen en in de back-up locatie kan schrijven. Via de taakplanner laat je het maken van de back-up uitvoeren onder dat aparte back-up-account. Zo ben je beschermd tegen malware die jouw data wil versleutelen. Of gebruik een back-up programma in de cloud zoals **KPN back-up online**[10] (€ 87,12 per jaar. Onbeperkt in omvang; één pc en … privé versleuteling) of **Livedrive** via backupmypc.nl[11] (€ 25,- per jaar; onbeperkt in omvang; onbeperkt in aantal pc's). Ook dan ben je veilig voor cryptolockers en tevens beveiligd tegen dataverlies bij brand of diefstal. Het geniet mijn voorkeur om geld uit te geven aan een goede back-up-oplossing boven een betaalde virusscanner.
De effectiviteit van de plug-ins en browsers kun je ook testen.
Kijk daarvoor op de site van **Panopticlick**[12].

Links

1 Social Engineering	http://bit.ly/wiki-soce
2 HitManPro Alert	http://bit.ly/sr-hmp
3 Adblock Plus	http://bit.ly/plugin-abp
4 AdBlock Plus Ads	http://bit.ly/abp-ads
5 NoScript	http://bit.ly/plugin-ns
6 Scriptsafe	http://bit.ly/plugin-ss
7 Ghostery	http://bit.ly/plugin-ghost
8 ADWcleaner	http://bit.ly/r-adwcleaner
9 HitManPro	http://bit.ly/r-hmp
10 KPN bu	http://bit.ly/kpn-bo
11 Backupmypc	http://bit.ly/r-bumpc
12 Panopticlick	http://bit.ly/r-potc
Dit artikel + links	http://reindjong.nl/browserbeveiliging
Mijn eigen site	http://reindejong.nl
Alle links als bundel	http://bit.ly/browserveilig