Windows 7/8 en veiligheid

Rein de Jong (Rhino)

Al eerder schreef ik over veiligheid. Met het verstrijken van de tijd zijn de gevaren veranderd en de tegenmaatregelen aangepast. Bedreigingen zijn doortrapter geworden en in aantal toegenomen. Slimme criminelen bedreigen ons. Zij vinden steeds weer nieuwe wegen naar onze pc's, die niet per definitie worden beveiligd. Zelf zullen we dus steeds meer alert moeten zijn! Deze verhandeling gaat over de gevaren die ons bedreigen en over wat we kunnen doen onder Windows 7/8 om zo veilig mogelijk bezig te zijn.

Veiligheid beperkt zich niet tot Windows 7/8. Het reikt verder dan dat. Ons eigen gedrag is mede bepalend. Vergeet niet dat we in de grote boze buitenwereld zijn, ook al zitten we thuis. Doordat we ons vaak in onze eigen vertrouwde omgeving bevinden, wanen we ons veilig. Dit is op zijn zachtst gezegd misplaatst!
Ruud Uphoff heeft ooit al eens een artikel geschreven over veilig gebruiken van de pc. Ik zal daar zoveel mogelijk op aansluiten of naar verwijzen.

Bedreigingen

PC en internet hebben ons veel zegeningen gebracht. Denk aan contacten, vrijheid, kennis en het samen werken aan projecten. Op het net zijn echter ook gevaren die ons bedreigen. Over het algemeen is het met de beveiliging van de computer en de internetverbindingen slecht gesteld. Onbeschermd het internet op en je pc is binnen minuten gekraakt! Tijdens een tv-uitzending werd een onbeveiligde pc met het internet verbonden. Binnen vier minuten was de eerste hacker binnen! Na een kwartier waren er drie hackers actief.
Zelf zijn wij echter de grootste bedreiging voor de pc. Door het per ongeluk wissen, niet beschermen van originelen, overschrijven van bestanden, gebruik van recoverydiscs, een datafout of defecte hardware, berokkenen wij de meeste schade. We moeten ons dus allereerst beschermen tegen onszelf. Pas dan komen de virussen en andere malware in zicht. Ook voor hackers ben je een makkelijke prooi.

Denk nu niet: 'Dat overkomt mij niet; ik ben niet interessant genoeg om te hacken.' Dat ben je wél! Er is namelijk geld mee te verdienen! En overal waar geld te verdienen valt, zijn er kapers op de kust! Binnen het hackerswereldje wordt per dag 1,5 miljard euro omzet gegenereerd! Momenteel wordt er 2,5 eurocent per gekraakte pc betaald. Voor gestolen Nederlandse of Belgische creditcardgegevens wordt 4 euro betaald. Voor Amerikaanse creditcards 6 cent!
Ook je identiteit is geld waard. Je identiteit kan worden 'gestolen' door wat je aan gegevens achterlaat op het web. Wanneer ook nog eens je pc wordt gehackt, is het al helemaal kinderlijk eenvoudig. Die gestolen identiteit kan worden gebruikt om leningen af te sluiten, goederen te bestellen, een B.V. op te richten, e.d. Het zal je maar gebeuren. Ook een dreiging is het gebruiken van je processor en schijfcapaciteit. Bijv. door het verhuren daarvan. Zo kan je pc opeens in een kinderpornonetwerk opgenomen worden. En als er iéts is wat je niet wil …

Door het verschuiven van toepassingen van de locale pc naar het web (Cloud-Computing) nemen dreigingen toe. Ook deze toepassingen maken het makkelijker om informatie over ons in te winnen en zijn potentieel een doel voor kwaadwillenden. Immers wanneer zo'n dienst een fout maakt, kunnen de door ons toevertrouwde gegevens zomaar op straat komen te liggen. Of erger, men kan er wijzigingen in aanbrengen. Door het verschuiven van de toepassingen van de desktop naar het web worden de browsers (Internet Explorer, FireFox, Chrome, Safari, etc.) een nog groter doelwit. Denk hierbij ook aan de invoegtoepassingen en andere uitbreidingen voor de browsers. Ook daar kunnen kwetsbaarheden in zitten. Met name pdf- en flash- uitbreidingen, die in praktisch elke browser zitten, zijn een dankbaar doelwit.

Hoe ons te beschermen?

Wat kunnen we tegen al die bedreigingen doen? Allereerst organisatorische maatregelen: de rol van de gebruiker. Daarbij valt te denken aan:

- Veiligstellen van gegevens (back-up)
- Gevaar niet uitlokken
- Kies verschillende mailadressen
- Wees wijs met wachtwoorden
- Sluit je netwerk af voor kwaadwillenden
- Dicht lekken in de software

Naast organisatorische maatregelen kan software een rol vervullen in het beveiligen van je gegevens. Het zijn maatregelen die je pc trager maken. Het zijn poortwachters. Vergelijk het met de veiligheidsdienst en douane op Schiphol. Hoe veiliger je de pc wenst te maken, des te meer tijd het kost om gebruik te maken van de nuttige dingen die je met de pc wenst te doen. Het is altijd een afweging tussen veilig willen werken en gebruiksgemak. Welke programma's kunnen het werken met de pc veiliger maken:

- Antivirusprogrammatuur
- Antispywareprogramma
- Antirootkit
- Antiphishingprogramma
- Firewall

Zorg wel, dat je UAC van Windows 7/8 in de hoogste stand hebt staan en niet als administrator werkt. Wanneer jezelf

alert bent en wanneer je niet op louche sites komt, dan kun je eigenlijk zonder al die softwarematige tegenmaatregelen. Resultaat: een heerlijk snelle pc!

Voorzorgsmaatregelen

Back-up
De meest universele voorzorgsmaatregel is de back-up. Deze vrijwaart ons van dataverlies. Dataverlies is iets vreselijks. Je zult maar een artikel, verweerschrift of de foto's van je pasgeboren (klein)kind kwijt zijn! Een (brand)veilig opgeborgen back-up, mits goed en regelmatig uitgevoerd, behoedt je daarvoor. Wees niet te zuinig en investeer in een goede back-up-voorziening. Combineer een aantal technieken. Het vreemde is dat 85% van de gebruikers zelden of nooit een back-up maakt. Zeker vreemd wanneer je weet dat 40% van de mensen allerlei persoonlijke informatie op de pc van onschatbare waarde vindt.
Een back-up maak je in ieder geval van je persoonlijke gegevens:
- Mijn Documenten
- Foto's
- Programma-instellingen/sleutels
- Favorieten
- E-mail en adresboek

Op:
- Netwerkschijf, DVD, Externe harde schijf, internet

Met gratis programma's zoals:
- Windows 7/8 back-up
- SyncBackSE free
- Picasa back-up
- Rsync back-up

Lok het gevaar niet uit
Doordat we vaak vanuit de vertrouwde omgeving werken, hebben we een misplaatst gevoel van veiligheid. Net als in de gewone omgeving zijn er op het internet veilige en onveilige omgevingen. Je kunt je voorstellen dat de kans om een trojan-horse te krijgen op de site van hema.nl kleiner is dan wanneer je op zoek gaat naar muziek en programmatuur. Zeker wanneer het illegale programmatuur/muziek betreft. Dus weet waar je surft! Download alleen vertrouwde en betrouwbare software! Laat je ook niet verleiden door angst. Raak niet in paniek wanneer opeens in je browser staat dat je besmet bent en programma XYZ zou moeten downloaden om je te beschermen. Vorig jaar zijn veel mensen besmet geraakt door nep-antivirussoftware (Bijv: XPsecurity-Center en VirusRemover 2008).
Versleutel vertrouwelijke gegevens.
Windows 7/8 Professional en Ultimate kunnen dat van huis uit (EFS-encryptie). De andere versies moeten hun toevlucht zoeken tot andere programma's. TrueCrypt is daarvoor een prima kandidaat.
Beperk ook je rechten. In Windows 7/8 is het eenvoudig om als gebruiker met beperkte rechten te werken. Moet er dan iets gebeuren waarvoor beheerderrechten noodzakelijk zijn, dan geeft UAC (dat natuurlijk in de hoogste stand staat) een waarschuwing en de mogelijkheid

om het wachtwoord van de beheerder in te voeren. Kwaadaardige software meldt zich dan ook en kan nergens bij! Werk dus minimaal met 2 accounts. Eén als beheerder en één of meer gebruikers met beperkte rechten!

Verschillende e-mailadressen
Scheiden van je adressen voor verschillende doeleinden voorkomt spam en andere ongewenste mail. Vluchtige e-mailadressen dragen bij aan het vermijden van ongewenste sporen. Maak verschillende aliassen voor:
- vrienden en bekenden
  - piet.janssen@hcc-net.nl
- bedrijven
  - meneer-pjanssen@hcc-net.nl
- nieuwsbrieven
  - nwsbfr.janssen@hcc-net.nl
- op het internet
  - inet.janssen@hcc-net.nl
- of een vluchtig adres:
  - xx uur: spambox (my-spambox plugin voor firefox)
  - xx mailtjes: spamgourmet.com

Gebruik daarnaast een spamfilter. Naar mijn idee een taak voor de provider. Doet die dat niet, dan is Thunderbird een goed e-mailprogramma met ingebouwd spamfilter of kijk eens naar Spamfighter.

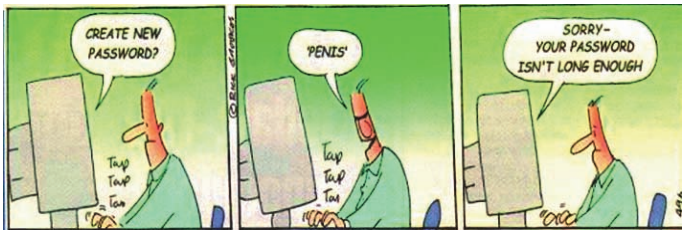
Wees Wijs met Wachtwoorden

Het is makkelijk om één simpel wachtwoord te hebben voor alles en nog wat. Veilig is dat niet! Je kunt je voorstellen dat een wachtwoord, dat zowel voor bankzaken als voor Hyves wordt gebruikt, niet veilig is. Eenmaal gekraakt ligt er veel voor de kraker open. Neem dus verschillende wachtwoorden voor verschillende veiligheidsniveaus. Gebruik verschillende tekens en maak het wachtwoord minimaal 10 tekens lang. Lengte is belangrijker dan tekenset. Wijzig regelmatig je wachtwoorden die gevoelige informatie beschermen. Gebruik op internet andere wachtwoorden dan lokaal. Laat die wachtwoorden verschillen per site! Neem voor internet een raamwerk. Bv. ww_deel1_xxx_deel2. Dat xxx verschilt dan per site. ww_deel1_hv_deel2 voor Hyves; ww_deel1_mp_deel2 voor Marktplaats. Voor _echt_ veilige wachtwoorden liever nog wat anders. Want wanneer iemand 3 of meer wachtwoorden van je in handen heeft, is het systeem zo achterhaald.

Gebruik voor je wachtwoorden een veilig programma om ze op te slaan. Voorbeelden hiervan zijn PINs en KeePass. Beide zijn al eerder door mij beschreven. Zie eerdere uitgaven of mijn site.
Een wachtwoordkluis is mooi, maar … wanneer er een keylogger op je systeem actief is, tja, dan heeft hij zo het wachtwoord van KeePass of een andere kluis te pakken en dan liggen al je wachtwoorden te kijk.

Ik vertrouw NU op mijn hoofd:
- Twee willekeurige tekenreeksen: een korte van zes tekens voor onbelangrijke/onbetrouwbare sites; een lange van tien tekens voor belangrijke gegevens;
- Aanvullen met tekens op bepaalde plekken die belangrijk zijn voor de ontsleutelplek. Denk hierbij aan een afkorting voor die plek en aantal tekens plus of min een waarde, etc.

Zo stamp je heel snel honderden wachtwoorden in je hoofd.



En die tekenreeks gebruik je een tijdje als je schermwachtwoord. Na een paar dagen vergeet je die nooit meer!

Dicht je netwerk
Indien mogelijk alleen een bekabeld netwerk gebruiken en dat voorzien van een goede hardwarematige firewall van de router, server of de provider. Naast het feit dat een bedraad netwerk sneller is, is het moeilijker te kraken. Je moet immers fysiek toegang hebben om het te kunnen tappen. Een draadloos netwerk is altijd af te tappen. In eerste instantie ziet de tapper alleen versleutelde gegevens. Die zijn te kraken! WEP versleuteling binnen de minuut! WPA/TKIP in een paar minuten. WPA-2 duurt erg lang, maar is ook te kraken. Een aantal KPN-routers met WPA-2/TKIP is ook in minuten te kraken door een configuratiefout. Ook hierover is al eerder een artikel in de SoftwareBus verschenen.
De firewall in de router moet zo worden ingesteld dat de poorten op stealth staan. Stealth wil zeggen: onzichtbaar. Dat is beter dan gesloten. Een gesloten poort nodigt uit tot inbreken. Een verborgen poort loop je voorbij. Testen bij www.grc.com.

Dicht lekken in de software
Internet-inbrekers gebruiken bekende achterdeurtjes en lekken die in de software zitten. Zodra er een lek wordt ontdekt, wordt software geschreven (botjes) die op zoek gaan naar kwetsbare pc's . Draai daarom regelmatig updates! Windows 7/8 staat zo ingesteld dat het regelmatig updates voor Microsoft-producten binnenhaalt en installeert. Laat zo mogelijk de standaard instellingen staan. Dat is: automatisch ophalen en installeren. Maar niet alleen Microsoft-updates installeren. De belangrijkste programma's die je moet updaten zijn:
- virusscanner
- browser (FireFox, Safari, etc.)
- Adobe Reader en Flash Player
- Java Runtime Environment

Om te weten of er gevaarlijke lekken zijn, kun je een abonnement nemen op de bulletins van de waarschuwingsdienst.nl en virusalert.nl.

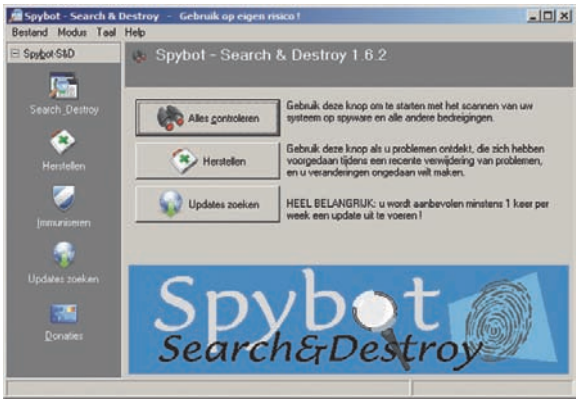
Rol van de software
Antivirusprogrammatuur Is je hoofdbeveiliging! Het programma moet alle bestandsingangen (bijv. Download-, Temp- en Windows-map) op de pc bewaken en aanslaan wanneer een programma iets wil doen dat niet door de beugel kan. De meeste malware wordt afgevangen op basis van herkenningsbestanden. Daarin staan tekenreeksen/opdrachtsignaturen die als verdacht zijn aangemerkt. Daarnaast kan een aantal antivirusprogramma's ook scannen op basis van heuristiek. Dat wil zeggen dat er naar verdacht gedrag (bedreiging/risico) van een programma wordt gekeken. Op basis daarvan wordt ingeschat of het al dan niet een virus kan zijn.

Je kunt je voorstellen dat deze wijze van analyseren tot foutieve conclusies kan leiden (zgn. false positives). Het scannen van e-mail, beveiligen van je browser en dat soort dingen vind ik onnodig. De meeste fabrikanten van antivirusprogrammatuur willen je dat, appelerend aan angst, wel graag verkopen, maar het is onnodig.
Het scannen van de mail is m.i. een taak van de providers. Hoe meer zij vangen voordat het verspreid wordt, des te meer bandbreedte is er over voor nuttige zaken. Immers, als een basisscanner aanslaat wanneer een virus zich op de harde schijf wil nestelen, is dat vroeg genoeg. Waarschijnlijk had je het bewuste mailtje voordien zelf al verwijderd. Je bent toch niet gek! Ook die heuristiek hoeft van mij niet zo. Een scanner op basis van actuele handtekeningbestanden, gecombineerd met UAC van Windows 7/8 in de hoogste stand, geeft afdoende veiligheid.
Je dient je namelijk af te vragen waarom UAC je toestemming vraagt. Is dat een toevallige actie of een actie die je zelf in gang hebt gezet (zie ook het artikel van Ruud Uphoff in SoftwareBus 2009-6).

Goede gratis antivirusproducten zijn (in alfabetische volgorde):
- Avast Home (NL)
- AVG Antivirus Free (NL)
- Avira Antivir
- Microsoft Security Essentials (NL)
- Panda Cloud Antivirus

Mijn persoonlijke voorkeur gaat uit naar Avira Antivir omdat het de minste systeembronnen gebruikt en hogelijk configureerbaar is. Als goede tweede zie ik Microsoft Security Essentials.
Scan ook af en toe eens met een tweede product. Alleen scannen. Niet installeren! F-Prot voor DOS of een online-scan van Kaspersky of Eset. Virusscanners scannen standaard alle bewegingen die op de harde schijf plaats vinden. Ook die gebieden waarvan je zelf wel weet dat er geen virus is. Zoek in de configuratie van de scanner naar de instelmogelijkheden en sluit die gebieden van on-access (bij toegang) scanning uit. Denk hierbij aan: mijn documenten, program files, foto's, muziek, films, en wat je nog meer kunt bedenken.

Antispyware
Deze 'tak van sport' wordt meer en meer óók door de antivirusprogramma's uitgevoerd. Windows 7/8 is standaard uitgerust met Windows Defender. Dat wordt na installatie van MSE uitgeschakeld omdat MSE die taak voor zijn rekening neemt. Ook wanneer je een andere virusscanner of antispyware programma in gebruik neemt is het goed om na te gaan of het de functie van Defender wellicht ook vervult. In dat geval Windows Defender uitschakelen! Start Windows Defender > Hulpprogramma's > Opties > Opties voor beheer > Verwijder het vinkje bij: 'Windows Defender gebruiken' > Klik opslaan.



Wil je heel graag een apart antispyware programma, kijk dan eens naar de gratis Spybot. Installeer dan niets resident. Dan worden zaken dubbel gecontroleerd en dat vertraagt de pc nodeloos. Alleen maar af en toe een totale scan met Spybot uitvoeren nadat de handtekeningbestanden zijn bijgewerkt.

Anti-rootkit
Rootkits zijn een set tools die zich diep in het systeem nestelen met als doel het aanmaken en verbergen van verbindingen en bestanden. In het nieuws gekomen doordat zelfs Sony zich aan

het gebruik hiervan schuldig maakte. Voordat een rootkit zich kan nestelen, heeft al iets kwaadaardigs toegang tot het systeem verkregen. Een goede virusscanner houdt dat tegen.

Het voorkomen van een rootkit is de taak van de virusscanner. Anti-rootkits zijn detectiemethoden. Ze werken niet proactief, zoals een virusscanner. Een rootkit is zeer moeilijk te verwijderen zonder het systeem te beschadigen. Vaak rest niets anders dan het systeem opnieuw te installeren. Het is niet eenvoudig om een anti-rootkit-programma te gebruiken. Voorbeelden van goede anti-rootkit programma's zijn: RootKitRevealer van Sysinternals en F-secure Blacklight.

Firewall
De firewall is ook bij het dichten van het netwerk al summier beschreven. Bij de software moet ik het ook aanstippen. De firewall van Windows blokkeert het inkomende verkeer en vraagt je om toestemming wanneer een nieuw programma naar buiten wenst te gaan. De firewall kan in hoge mate worden geconfigureerd. Hiervoor is echter een gedegen kennis van TCP/IP en netwerkpoorten noodzakelijk. Doe er alleen wat mee wanneer je die kennis hebt en weet wat veilige processen zijn. Voor het normale verkeer zijn de standaard instellingen meer dan voldoende.

Bedenk ook hier dat je moet voorkomen dat malware binnenkomt. Is het eenmaal binnen en heeft het beheerrechten, dan helpt niets meer. De malware is immer almachtig op je systeem.

Betekenis voor Windows 7/8
Hoe geldt het voorgaande voor Windows 7/8? Wat kun je er dan mee? Relevante Windows 7/8-raakpunten zijn hiervoor al genoemd. Samenvattend kan worden gesteld dat Windows 7/8 afdoende is beschermd met:

- zijn eigen firewall in de standaard instelling;
- Gebruikers Account Beheer (UAC) in de hoogste stand te plaatsen;
- het werken als een standaard gebruiker;
- het installeren van een basale virusscanner;
- een regelmatige back-up van je eigen gegevens.

De keuze voor een virusscanner onder Windows 7/8 is niet eenvoudig. De scanners zijn steeds aan het stuivertje wisselen. Nu eens is Avira de beste, dan weer komt Avast als beste uit de bus. Op dit moment, voorjaar 2013 komen de volgende scanners als beste uit de test volgens www.AVtest.org.

- Gratis Scanners:
  1. Avast free
  2. AVG free
  3. Avira free

- Betaalde scanners:
  1. AVG
  2. Bitdefender
  3. Eset

Ik ben geen voorstander van de uitgebreide pakketten. De firewall van Windows is immers prima en je hebt er geen omkijken naar. Dat is bij de totaalpakketten wel anders! Altijd sores. Vergeet niet dat, ook bij de keuze van een scanner, er een afweging moet worden gemaakt tussen nut en noodzaak, tussen overlast en gebruiksgemak. Geen enkele scanner biedt 100% veiligheid. Je eigen waarneming is de beste scanner die je hebt. De beste scanner zit tussen je oren!

Zoveel is er dus gelukkig niet nodig. Windows 7/8 is een robuust en veilig besturingssysteem!

Veiligheid: een kwestie van balans
Altijd afwegen: wat is veilig en wat is werkbaar. Doe het VVV: Veilig, Verstandig en Voorzichtig. Met die drie woorden is eigenlijk alles gezegd. Met dat motto blijft je systeem werkbaar. Bedenk dat met drie sloten op je deur plus een alarmsysteem het woongenot beperkt is. Zo ook het installeren van veel veiligheidsprogramma's op je computer.
Wees alert wanneer je op het internet zit. Dat is de boze buitenwereld; je ben niet thuis!

Vragen
Mocht u naar aanleiding van deze artikelen vragen hebben, dan kunt u deze, als lid van de HCC, stellen in de forums van de HCC. HCC!forums kunt u vinden op www.hccforums.nl. Er is zelfs een speciaal Expertforum voor Windows 7/8; daarin geef ik ook antwoorden. Of kijk ook eens op mijn website: www.reindejong.nl

www.reindejong.nl

Bronnen & Links:

- www.waarschuwingsdienst.nl
- www.govcert.nl
- trendrapport 2009: Cybercrime in trends en cijfers
- www.security.nl
- 3xkloppen.nl
- TrueCrypt - www.truecrypt.org
- Avira - www.free-av.com
- mijn eigen site: www.reindejong.nl