

Beveiligingstest 1 - aanvulling

Is uw pc up-to-date volgens Windows update?

Eén van de basis elementen met betrekking tot het beveiligen van uw pc is vanzelfsprekend dat uw besturingssysteem voorzien is van de nieuwste updates zodat de bekende veiligheidslekken gedicht zijn. Het gaat in dit geval om de zogenaamde 'essentiële updates' oftewel updates die van groot belang zijn.

Indien u uw pc heeft ingesteld op het automatisch installeren van deze updates dan krijgt u vanzelf een melding van uw pc wanneer de betreffende updates zijn gedownload en klaar staan voor installatie. U kunt ook zelf de [website van Microsoft](#) bezoeken om de nieuwste updates binnen te halen.

Iedere eerste dinsdag van de maand is er een zogenaamde 'Patch Tuesday' en worden er meestal een aantal belangrijke updates uitgebracht. Wilt u deze updates dus snel hebben dan kunt u op zo'n 'Patch Tuesday' zelf de website bezoeken en de updates binnen halen. Vergeet enkel niet dat tussentijds ook belangrijke updates kunnen verschijnen.

De makkelijkste methode om direct te weten wanneer er essentiële updates verschijnen is simpel; [registreer](#) op ons forum en meld u aan bij de groep 'Mailinglijst'. U ontvangt dan per e-mail iedere essentiële updates inclusief uitleg en installatie instructies, zowel van Microsoft als van andere leveranciers (bijv. Adobe, Flash, etc.).

Is uw pc up-to-date volgens UpdateChecker?

Buiten software van Microsoft staat er op de gemiddelde pc nog veel meer software waar regelmatig updates voor uitkomen. De meeste programma's regelen dit zelf door na het opstarten even te controleren op updates. Maar niet alle programma's zijn automatisch voorzien van de nieuwste updates. Soms zijn dit programma's die u niet handmatig opstart, maar die wat meer op de achtergrond meedraaien.

Om al die software te controleren op eventuele updates heeft Hipposoft het programma '[UpdateChecker](#)' uitgebracht. Hiermee wordt niet alleen gekeken voor welke programma's updates beschikbaar zijn, maar er wordt zelfs een keurige lijst gepresenteerd met alle beschikbare updates inclusief een download-knop. U hoeft dan enkel de download te installeren (openen i.p.v. opslaan) en het betreffende programma is up-to-date.

Gebruikt u een bekende virusscanner?

Het installeren van een [goede en bekende virusscanner](#) is eveneens een basis vereiste voor de veiligheid van uw pc. Zonder deze software hebben virussen, wormen, trojans etc. vrij spel op uw pc.

Men beweerd wel eens; *"Ik heb geen virusscanner en nooit last van virussen"*, meestal komt dat juist doordat de betreffende virussen, wormen en trojans niet ontdekt worden en zich ook niet bekend maken op de pc (deze malware wil natuurlijk 'stiekem' aan de slag). Virusscanners zijn zowel betaald als gratis te verkrijgen en halen vrijwel allemaal automatische de nieuwste updates (herkenningslijsten) binnen. U dient wel periodiek de pc te scannen, maar ook dat kunt u eventueel automatisch laten doen.

Gebruikt u een firewall?

Ook het hebben van een [goede en bekende firewall](#) is één van de basis elementen van een veilige pc. Zoals een virusscanner controleert op kwaadaardige bestanden, zo controleert een firewall op kwaadaardige verbindingen (internetverkeer) van en naar uw pc. Vanaf het internet worden aanvallen uitgevoerd op uw pc om deze geïnfecteerd te krijgen. Een goede firewall herkent en blokkeert deze aanvallen. In tegenstelling tot de virusscanner zit de firewall wél standaard in Windows (Beveiligingscentrum). Deze Microsoft firewall is niet één van de beste, maar kan voldoen voor een basisbeveiliging. Het grote nadeel van deze standaard firewall is dat deze alleen het inkomende internetverkeer controleert op kwaadaardige code, indien uw pc besmet is met malware die zelfstandig verbinding maakt met kwaadaardige computers op het internet dan is dat uitgaand internetverkeer en wordt dat dus niet waargenomen! Nadeel van de meeste firewalls is dat het enigszins ingewikkeld kan zijn om alle instellingen juist te zetten. Als u bijvoorbeeld online spellen speelt worden deze soms geblokkeerd door de firewall, u dient dan aan te geven dat het om goedaardig verkeer gaat.

Gebruikt u de nieuwste versie van uw browser?

Uw browser (Internet Explorer, Firefox, Google Chrome etc.) is het kanaal tussen u en het internet. Het is dus van belang dat deze browser van de nieuwste updates wordt voorzien. Andere software kan eventueel een tijdje wachten op het installeren van een update, maar aangezien de browser direct met het internet communiceert dient deze zo up-to-date mogelijk te zijn. Vaak worden zogenaamde 'patches' (updates) uitgebracht om een specifiek beveiligingslek wat misbruikt wordt te dichten.

De vraag welke browser het beste (lees: veiligst) is kan leiden tot ellenlange discussies. Meestal wordt deze keus gebaseerd op persoonlijk voorkeur. Internet Explorer is nog steeds de meest gebruikte browser (temeer omdat Microsoft deze [voorlopig nog] standaard bij Windows levert) maar Firefox van Mozilla krijgt steeds meer marktaandeel, groot voordeel van Firefox is dat met behulp van honderden 'plug-ins' (lees: uitbreidingen) deze browser volledig aan te passen is.

Gebruikt u een anti-malware programma?

Malware is een verzamelnaam voor kwaadaardige en/of schadelijke software. Het woord is een samenvoeging van het Engelse *malicious software* (kwaadwillende software). Het is altijd verstandig om naast de standaard virusscanner een Anti-Malware programma te hebben. Aangezien vrijwel geen enkele virusscanner alle virussen detecteert, kan een goed Anti-Malware programma een doeltreffende aanvulling zijn hierop. Risico is wel dat er meer dan genoeg nepprogramma's rondzwerven, die (onterecht) aangeven dat de pc besmet is en meteen een downloadlink geven voor het betreffende programma waarvoor vaak ook nog betaald moet worden. Meestal is wel te zien dat het om een nepprogramma gaat, maar sommige zien er behoorlijk realistisch uit. Eén van de betere, zonet het beste, Anti-Malware programma's is [MalwareBytes' AntiMalware](#). Op de site vindt u een [handleiding](#) van dit programma..

Scant u regelmatig uw pc?

Het is aan te raden om met regelmaat de pc te scannen, hoe vaak dit dient te gebeuren is afhankelijk van uw eigen gevoel, de manier waarop u uw pc gebruikt (bijv. veel downloaden) en de waarde van de gegevens op uw pc (financiële gegevens of andere waardevolle bestanden). Bij normaal gebruik volstaat het om één maal per maand een scan uit te voeren. Zorg eerst dat al uw software up-to-date is, zowel Windows zelf als de overige software. Start daarna uw virusscanner of Anti-Malware programma op, controleer of deze over de nieuwste virusdefinities beschikt en voer een volledige scan uit (i.p.v. snelle scan). Zorg ook dat eventuele extra harde schijven aangevinkt staan en dus in de scan worden meegenomen. Eventueel kunt u eenmaal per maand een volledige onderhoudsbeurt laten plaatsvinden. Dan bestaan de handelingen uit bijv.; updaten, scannen, foutopsporing, defragmentatie, opruimen, back-uppen en dergelijke.

Gebruikt u sterke wachtwoorden?

Des te meer tijd u op de pc doorbrengt, des te meer wachtwoorden u gaat gebruiken. Het beste is om overal verschillende wachtwoorden voor te gebruiken. De wachtwoorden zelf dienen ook 'kraakbestendig' te zijn;

- 1) gebruik minimaal 8 tekens.
- 2) gebruik, naast letters, ook cijfers en overige tekens (#]*&=€)
- 3) gebruik geen woorden uit het woordenboek
- 4) combineer hoofdletters met kleine letters
- 5) Bewaar geen lijst met wachtwoorden op uw computer

Op de website treft u [meer informatie](#) over wachtwoorden aan, tevens kunt u daar uw wachtwoord laten controleren op sterkte.

Er zijn programma's in omloop die alle wachtwoorden opslaan (bijv. Roboform) en zelfs automatisch kunnen inloggen op websites, fora en dergelijke. Voordeel hiervan is dat u geen wachtwoord meer kunt vergeten en dat het inloggen automatisch gebeurt. Deze programma's bewaren alle wachtwoorden versleuteld zodat kwaadwillende hier niet bij kunnen, het is wel aan te raden om de lijst af en toe te back-uppen of uit te printen.

Is uw modem/router goed beveiligd?

Los van de beveiliging van uw pc dient u tevens uw modem en eventueel uw router te beveiligen. De beveiligingsmogelijkheden verschillen enorm per modem/router. Zo is de Experia-box van KPN niet bijzonder gebruiksvriendelijk en bieden de routers van bijvoorbeeld Sitecom juist weer enorm veel mogelijkheden. Het is niet in een paar woorden te beschrijven hoe deze beveiliging het beste in te stellen is. In het kort komt het erop neer dat draadloos onveiliger is dan bedraad, dat draadloos het beste beveiligd is met WPA2-AES en dat men zo snel mogelijk na aankoop het wachtwoord dient te veranderen. Een uitgebreidere [handleiding](#) met betrekking tot het beveiligen van draadloze netwerken vindt u op onze website.

Let u op met wat
u aanklikt/download?

Het belangrijkste onderdeel; u als gebruiker.. Wat voor beveiliging u ook heeft, u bepaalt wat er geïnstalleerd, gedownload of bezocht wordt. Ga af op uw gevoel, neem het zekere voor het onzekere in geval van twijfel en gebruik programma's als McAfee SiteAdvisor om alle websites te voorzien van een veiligheidslabel. Download en scan bestanden voordat u deze installeert. Laat u niet overhalen door pop-ups en nepameldingen om zogenaamde scanners te kopen.

Copyright 2009 www.pcbeveiligen.nl

Niets uit deze uitgave mag worden verspreid of gekopieerd zonder
behoud van de oorspronkelijke bronvermelding (www.pcbeveiligen.nl)