DOSgg op HCC-dagen

De HCC-dagen zijn een begrip in Nederland. Alle computeraars herinneren zich nog wel de verstopte wegen rond Utrecht. Traditioneel wordt deze driedaagse happening in de Jaarbeurs gehouden van vrijdag t/m zondag. Met soms meer dan 100.000 bezoekers. Vorig jaar werden de HCC-dagen wegens omstandigheden afgelast, maar dit jaar zijn ze er weer. Op 28, 29 en 30 november staan de deuren van de Jaarbeurs open. Dit jaar onder de naam HME (Hét Multimedia Event) 2008, een samenwerking van Magevents, Sanoma Men's Magazines, de HCC!dagen en de Hardware Info Dagen.

De DOS gebruikersgroep zal daar de grootste stand van alle HCC-groeperingen innemen. Op 150 m² presenteren DOSgg-Platforms (DigiFoto, DigiVideo, Windows, Netwerken, Linux, Muziek, VoIP, WebDesign), de DOSgg VraagBaak, de redactie van de SoftwareBus et cetera zich in levenden lijve en staan ze bezoekers te woord. Ook zijn er demo's en (korte) workshops. Voor leden van de DOSgg is er zoals vanouds altijd wat te halen. Naast gratis koffie en koek kun je op vertoon van de HCC-DOSgg-ledenpas dvd's en cd's meenemen. Voor niet-leden zijn deze verkrijgbaar tegen beursprijzen. Degenen die nog geen lid zijn van de DOSgg kunnen zich nog aanmelden op www.DOSgg.nl. Voor HCC-leden die nog geen gebruikers (interesse) groep in hun pakket hebben is dat gratis. Lid worden van de HCC kan al vanaf 10 euro per jaar. En dan krijg je gellijk 50% korting op de toegangsprijs van de HME-dagen! In het novembernummer van CHIP geven we meer details over dit evenement en de deelname van de hcc!DOSgg. Enne, zien we elkaar dan eind november onder het genot van een kopje koffie?

DOSgg VraagBaak

Loop je wel eens tegen een computerprobleem aan dat je hoopt op te lossen door naar het probleem te 'googelen'? Kom je dan 'oplossingen' tegen waarvan de ene nog slechter is dan de andere? Of dat je dan ineens een 'free download' moet binnenhalen à raison van € 39,95? Gelukkig is daar een heel goed alternatief voor! Op de website van de hcc!DOSgg (www.dosgg.nl) vind je bovenaan een link, genaamd DOSgg Helpdesk. Die helpdesk wordt bemand door experts (wij noemen ze VraagBaak) op allerlei gebieden, zoals de besturingssystemen Windows en Linux, maar ook officepakketten (zowel Microsoft als OpenOffice.org), fotobewerking, netwerken en beeldbewerking. Kortom, zo'n beetje alles wat je op computers kunt tegenkomen. Op de site is beschreven hoe je contact opneemt. Je kunt mailen of bellen. Heb je haast, dan bel je 0317-707 425. Via een keuzemenu word je naar de juiste VraagBaak geleid. Is het probleem niet urgent, dan mail je. De juiste mailadressen vind je op www.DOSgg.nl: het 'centrale' mailadres is VraagBaak@DOSgg.nl. Uit eigen ervaring weet ik dat je dan meestal binnen 24 uur antwoord krijgt. Je kunt vooraf eens kijken in het DOSgg-forum (http://forum.DOSgg.nl) of in de DOSgg Kennisbank (zie www.DOSgg.nl). Als eindredacteur van ons magazine SoftwareBus lees ik vooraf alles wat daarin geplaatst wordt. Kortgeleden zat daar een artikel bij van Ruud Uphoff, een VraagBaak van het eerste uur met een ontzaglijke hoeveelheid praktische kennis. In het artikel beschrijft Ruud de oplossing van een twaalftal veel voorkomende problemen. Onder meer hoe je ervoor zorgt dat je standaardbrowser een html-bestand kan openen als hij dat ineens niet meer doet. De dag nadat ik het gelezen had, werd ik benaderd door een kennis van mij die op zijn computer met precies dat probleem kampte. Uiteraard kon ik hem toen Ruuds oplossing toesturen. De dag daarna kreeg ik bericht dat de foute instelling met succes was gerepareerd. Bedankt Ruud!

Rob de Waal Malefijt

Laptop gestolen?

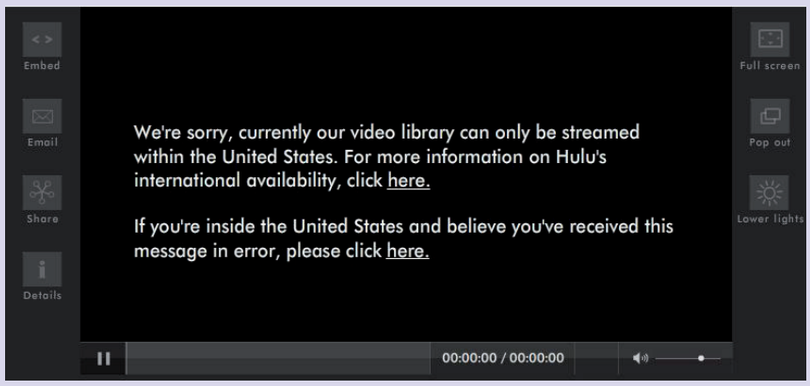
Mijn laptop en ik zijn onafscheidelijk. Totdat ik met mijn neus op de harde feiten werd gedrukt. Een nachtelijke treinreis door Oekraïne ging goed, maar bijna thuis op het station van Duivendrecht ging het toch mis. Je wordt een fractie van een seconde afgeleid en foetsie laptop. Werk weg, bestanden weg. De laptop werd een laptob.

Maar het ergste is dat je gegevens in handen van anderen zijn. Helaas worden beveiligingsmaatregelen zoals wachtwoord- of (biometrische) toegangscontrole en versleuteling te weinig toegepast. Toch is het verstandig het de dieven zo onaantrekkelijk mogelijk te maken een laptop te stelen. Na de diefstal gaat meestal de nieuwe (onrechtmatige) eigenaar het apparaat uitproberen. Aan een computer die niet opstart, heeft die dan niet zo veel. Tegenwoordig is geen computer meer zinvol te gebruiken zonder internet. En daar komt Laptop Cop te hulp. Zodra de gestolen laptop zich op internet begeeft, kan de rechtmatige eigenaar een verbinding maken. Zonder dat de onverlaat het merkt, worden kopieën van (belangrijke) bestanden verstuurd naar de eigen of een vertrouwde computer en kunnen de veiliggestelde bestanden van de laptop verwijderd worden. Maar daarmee houdt het speurwerk van Laptop Cop niet op. In het geheim worden handelingen van de 'nieuwe eigenaar' in een logboekbestand weggeschreven. Voorbeelden hiervan zijn: e-mails, adresboeken, bezochte websites, chatsessies, gebruikersnamen, wachtwoorden en dergelijke. Dit logboek wordt via internet verzonden en bewaard. De opsporing door de politie kan hiermee goed geholpen worden. Bovendien kunnen alle gegevens van de dief op het beeldscherm van de gestolen laptop gezet worden, in de hoop dat deze daardoor aangespoord wordt de laptop terug te bezorgen. Het idee van deze vorm van beveiliging is niet

nieuw en er zijn in het verleden al varianten op de markt gebracht, die bijvoorbeeld ip-adressen van de gestolen laptop doorgaven of wisacties in gang zetten. Of de software nog werkt als de harde schijf met Laptop Cop en al geformatteerd wordt, laat de maker van het programma wijselijk in het midden. Het programma is in Nederland verkrijgbaar bij www.pcsafe.nl voor circa € 37,- per jaar.

Hotspot Shield

WLAN kan veilig zijn, maar is dat vaak niet! Thuis is er vaak geen of onvoldoende beveiliging. Je weet dat WEP verre van veilig is, een beetje hacker kraakt dat in no time. Stel thuis daarom - als je apparatuur dat toelaat - altijd de WPA-beveiliging in, liefst WPA2. Onderweg zijn veel 'hotspots' onbeveiligd. Ja, je moet vaak inloggen met een naam en wachtwoord om toegang te krijgen waar je in de regel voor moet betalen. Maar vervolgens gaan je gegevens in 'klare taal' door de lucht. Iedereen kan die afvangen en lezen. Vooral hotspots in hotels, cafés en dat soort openbare gelegenheden zijn gevaarlijk. Je e-mails en creditcardgegevens liggen heel snel op straat. Zelfs je VoIP-gesprekken zijn af te luisteren. Skype is overigens standaard goed beveiligd. Hotspot Shield geeft een uitstekende oplossing voor de hotspots waar je tegen betaling mag inloggen, maar waar het dataverkeer onbeveiligd is. Het maakt gebruik van een VPN (Virtual Private Network) verbinding, een veilige 'tunnel', uiteraard met encryptie. De makers van Hotspot Shield hebben een gateway die je internetverkeer vervolgens (verder onbeveiligd) het internet op gooit. Tot aan deze gateway ben je anoniem (nou ja, behalve dan op de plek waar je het WiFi-netwerk op ging). Vanaf deze gateway zie je eruit als een vermomde Amerikaan en dat heeft voordelen. Je kunt zo veel Amerikaanse streaming sites bekijken, bijvoorbeeld www.hulu.com. Zoals je eigenlijk ook niet op de camping in Frankrijk via de satelliet naar de Nederlandse tv mag kijken. Dat heeft vaak te maken met copyrights. Bekabelde netwerken in openbare gelegenheden zijn vaak onveilig. Het kan maar zo gebeuren dat ergens in een hotel, zoveel verdiepingen hoger, je concurrent je internetverkeer zit mee te loggen. Ook daarvoor is Hotspot Shield een uitstekende oplossing. Hotspot Shield is gratis. Het gebruik is gratis, maar beperkt tot 3 gigabyte per 'voortschrijdende' maand. Dus niet bedoeld voor 'heavy leechers'. Alhoewel tegen betaling een account met hogere limiet mogelijk is. Op de DOSgg GigaHits 2008-04 (gratis dvd bij de SoftwareBus) staat Hotspot Shield, maar je kunt het ook downloaden van www.hotspotshield.com.



Streaming site www.hulu.com is alleen zichtbaar voor Amerikanen

The New eXPerience: Vista-look op XP

Is het echt nodig om over te stappen op Vista? Wel als je de buurman de ogen wilt uitsteken met die flitsende 3D aero-look, die je krijgt bij Vista Home Premium voor zo'n € 225. Waarom geld uitgeven als je kunt upgraden vanaf Windows XP?!

Vista Transformation Pack

Surf snel naar Windows X's Shrine (www.windowsxlive.net/vista-transformation-pack) om het Vista Transformation Pack 8.0.1 te downloaden. Het pakket is ruim 30 megabytes groot. Windows X's Shrine is trouwens best een interessante site voor de Windows-adepten. Er worden allerlei snufjes en verfraaiingen voor Windows uitgedokterd. Terug naar het Vista Transformation Pack. Nee, het maakt van XP geen Vista. Maar het doet wel alsóf. Daarmee is je hoofddoel meteen al bereikt: Je omgeving denkt dat je Vista hebt.

De installatie

De installatie van het pakket is heel simpel. Gewoon het (uitgepakte) bestand opstarten in de verkenner, alle vragen beantwoorden met 'yes' en alle hokjes die langskomen aanvinken. Tijdens het installeren krijg je allerlei mogelijkheden voorgeschoteld. Je kunt zelf bepalen wat er allemaal op Vista moet gaan lijken. In totaal kostte mij dat ongeveer tien minuten. Bezint eer ge begint: er wordt geadviseerd de nodige back-ups te maken.

Nieuwe kleren van de keizer

Laten we bij het begin beginnen. Na de installatie moet Vista... eh, nee.... XP dus... opnieuw starten. Het opstartscherm meldt zich niet langer met Windows XP, maar met Windows Vista. Tenminste, als je deze optie hebt aangevinkt tijdens de installatie. Na verloop van tijd verschijnt het bureaublad. Alle pictogramman lijken sprekend op die van Vista. Rechts zie de je de typische Vista-sidebar. Hoe die eruitziet, kun je zelf instellen. In de sidebar staan allerlei handige widgets. Dat zijn kleine programma's waarvan een aantal is meegeleverd en andere die je kunt downloaden. Je kunt kiezen welke gadgets je wilt tonen en de mate van doorzichtigheid instellen. Als je daar heel ver in gaat, zijn alle gadgets en pictogrammen 100 procent transparant. Ze zijn er dan nog wel, maar je ziet ze niet. Net als de nieuwe kleren van de keizer uit het sprookje. Schaduw, kleuren, scherpte: je kunt het allemaal instellen.

Conclusie

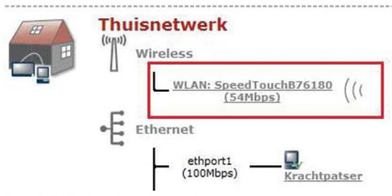
Met het Vista Transformation Pack 8.0.1 verander je het uiterlijk van Windows XP in dat van Windows Vista. Deels gedraagt het zich dan als Vista. De Vista-look met de sidebar past uitstekend op de moderne breedbeeldschermen. De sidebar neemt een stuk van de extra breedte weg en daardoor houd je toch weer een scherm met de gebruikelijke proporties over. Het opstarten van XP met het geïnstalleerde Vista Transformation Pack duurt wat langer omdat alle grafische toeters en bellen geladen moeten worden. De DOSgg heeft het vorig jaar al op de GigaHits gezet, de dvd die bij elke aflevering van het blad de SoftwareBus meegeleverd wordt. Versie 9 is al wel aangekondigd. Op GigaHits 2008-05 (verschijnt 29 oktober) zal een update opgenomen worden.

Onveilige KPN-modems!

Het DOSgg-lid Marius bracht het volgende onder de aandacht, zie http://forum.DOSgg.nl/showthread.php?t=9278. Een waarschuwing is op zijn plaats voor de gebruikers van de zwarte ExperiaBox of Speedtouch 780 modem, dat door KNP & Co (KPN, Planet , XS4ALL, HetNet, en andere) op grote schaal aan InternetPlusBellers en ADSL-abonnees wordt verstrekt. Een groot aantal van deze modems is af-fabriek voorzien van een beveiliging (WPA), die kinderlijk eenvoudig te vinden is. Het gaat met name om modems van het type Speedtouch 780 (waaronder de zwarte Experiabox). Het speelt niet bij de zilverkleurige Experiabox (van Siemens).
De modem zendt standaard zijn naam (SSID) uit in het draadloze signaal. Zo'n SSID kan in dit geval bijvoorbeeld zijn: Speedtouchxxxxxx (op de plaats van een x staat een ander teken). KPN/Speedtouch gebruikt(e) helaas standaard toegangscodes (combinatie SSID en WPA-key), die tot elkaar te herleiden zijn.

Die laatste zes tekens van het door KPN verstrekte SSID zijn dan, met een simpel programmaatje dat op het internet te vinden is, te herleiden tot de (meestal) door de KPN-ADSL-provider bij aflevering aangeleverde WPA-beveiligingscode. Als je daarna je WPA-code (en/of SSID) niet veranderd hebt, dan kan een kwaadwillende hiermee gemakkelijk toegang tot je internetverbinding (en je computer) verwerven. Desgewenst kun je die eventuele onveiligheid zelf vaststellen door die laatste zes tekens van het SSID los te laten op het programmaatje 'speedtouchkey.exe' dat je van internet haalt. Maar nog gemakkelijker gaat het op www.speedtouch.websijt.net.
Als dan jouw WPA-code in beeld verschijnt, weet je dat de beveiliging van je draadloos netwerk ondeugdelijk is. Verschijnt de juiste code niet, dan loopt jouw draadloze router in beginsel niet dit inbraakrisico. KPN zegt op haar site onder het kopje 'Veilig draadloos online': "KPN

heeft al haar modems goed beveiligd. Een draadloos modem van KPN is standaard voorzien van een beveiligingscode. Deze beveiliging zorgt ervoor dat de gegevens die tussen je modem en computer door de lucht gaan worden versleuteld." Dat klopt, maar een paar regels verderop staat dat kwaadwillenden deze beveiliging kunnen omzeilen. KPN raadt aan om de SSID (naam van je draadloos netwerk) te wijzigen, zodat herleiden van je WPA-code onmogelijk wordt. Een matig advies. Immers, ik zou de SSID-naam van mijn buurman al ergens genoteerd kunnen hebben! De Consumentenbond raadt op haar site aan om ook de WPA-code te wijzigen, zie http://tinyurl.com/6nglzz. En daar sluiten wij ons volledig bij aan. Je kunt het nog veiliger maken door de SSID te verbergen. Kijk ook de instellingen van je modem na als de KPN daaraan 'onderhoud' heeft uitgevoerd. Er zijn gevallen bekend waarbij de beveiliging door de gebruiker was gewijzigd, maar door de KPN-monteur teruggezet was op de (onveilige) situatie bij aflevering! Als je WiFi-netwerk niet of onvoldoende is beveiligd, kunnen derden je 'afluisteren', met alle gevolgen van dien. Er zou bijvoorbeeld via jouw aansluiting illegaal materiaal op het internet geplaatst kunnen worden. Dus nogmaals: altijd ten minste SSID en beveiligingssleutel wijzigen. En natuurlijk ook de inlognaam en wachtwoord om in de setup van de modem te komen. Niet alleen met de KPN-modems, maar altijd!



De SSID is zichtbaar in de setup, maar wordt ook voor iedereen zichtbaar uitgezonden!