HCC DOSgg

20 september: MegaGebruikersDag

In c't magazine van september hebben we al het een en ander verteld over deze manifestatie van de hcc!DOSgg en nog zo'n tien andere HCC-groepen. Inmiddels zijn er meer details bekend en kunnen we er al wat meer over zeggen.

Op www.DOSgg.nl staat een volledig en up-to-date overzicht van het programma. Demonstraties, lezingen, workshops en de DOSgg VraagBaak in levende lijve! De MegaGebruikersDag is op zaterdag 20 september van 10-16 uur in het H.F. Witte Complex, Henri Dunantplein 4, 3731 CL De Bilt.

Ook c't-lezers zijn van harte welkom. De toegang is gratis, je kunt komen en gaan zoals het je uitkomt. Wanneer deze c't in je brievenbus ligt, is er nog voldoende tijd om aan de hand van het programma je bezoek vooraf te plannen en optimaal de activiteiten 'mee te pikken' die het meest van je gading zijn. Alles bijwonen kan niet, want een aantal activiteiten vindt parallel plaats. Inschrijven voor de DOSgg Workshops hoeft niet meer, die zijn vast al volgeboekt.

Ook dit jaar brengt Microsoft weer het laatste Windows-nieuws.

HotSpot Shield

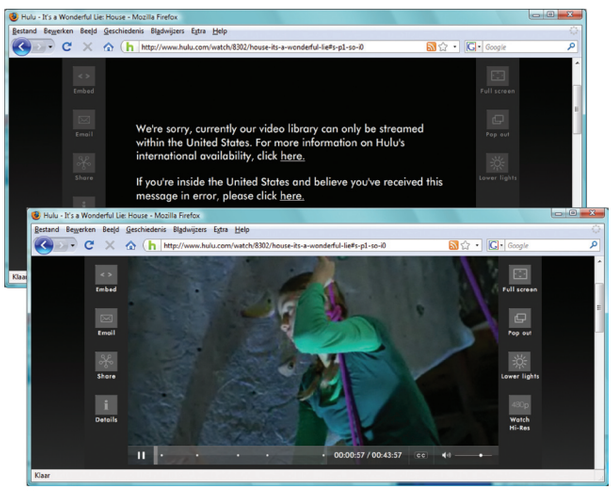
WLAN kan veilig zijn, maar is dat vaak niet! De meeste mensen hebben thuis vaak geen of onvoldoende beveiliging. Je weet dat WEP verre van veilig is, een beetje hacker kraakt dat in no time. Stel thuis daarom – als je apparatuur dat toelaat – altijd de WPA-beveiliging in, liefst WPA2.

Onderweg zijn veel 'hotspots' onbeveiligd. Je moet vaak wel inloggen met een naam en wachtwoord om toegang te krijgen, waar je in de regel dan voor moet betalen. Maar vervolgens vliegen je gegevens in 'klare taal' door de lucht. Iedereen kan die opvangen en lezen.

Vooral hotspots in hotels, cafés en andere openbare gelegenheden zijn gevaarlijk. Je e-mails en creditcardgegevens liggen heel snel op straat. Zelfs je VoIP-gesprekken zijn af te luisteren, al is Skype overigens standaard goed beveiligd.

Hotspot Shield is een uitstekende oplossing voor de hotspots waar je tegen betaling mag inloggen, maar waarbij je dataverkeer vervolgens onbeveiligd door de lucht gaat. 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 ben je vermomd als een Amerikaan. Dat heeft ook nog andere voordelen. Je kunt zo bijvoorbeeld veel Amerikaanse streaming sites bekijken, zoals www.hulu.com, die alleen voor inwoners van de USA toegankelijk zijn. Vaak heeft dat te maken met copyrights.



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

Ook bedrade netwerken in openbare gelegenheden zijn vaak onveilig. Het kan maar zo gebeuren dat ergens in een hotel, een aantal verdiepingen hoger, je concurrent je internetverkeer zit mee te loggen. Ook dan is Hotspot Shield een uitstekende oplossing.

Hotspot Shield is gratis. Het gebruik is ook gratis, maar wel beperkt tot 3 gigabyte per maand. Dus niet bedoeld voor 'heavy leechers'. Alhoewel tegen betaling wel een account met een hogere limiet mogelijk is.

Op de DOSgg GigaHits 2008-04 (gratis dvd-rom bij de SoftwareBus) staat Hotspot Shield. Maar je kunt het ook downloaden van www.hotspotshield.com.

Onveilige KPN-modems

Een gewaarschuwd mens telt voor twee. Het DOSgg-lid Marius heeft op ons forum een bericht gepost over de ondeugdelijke beveiliging van KPN-modems, zie http://forum.DOSgg.nl/showthread.php?t=9278

Deze waarschuwing geldt voor gebruikers van het 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.

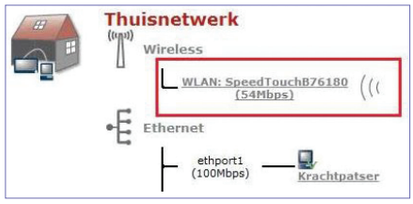
Een groot aantal van deze modems is af-fabriek voorzien van een beveiliging (WPA) waarvan de code kinderlijk eenvoudig te ach-

HCC DOSgg

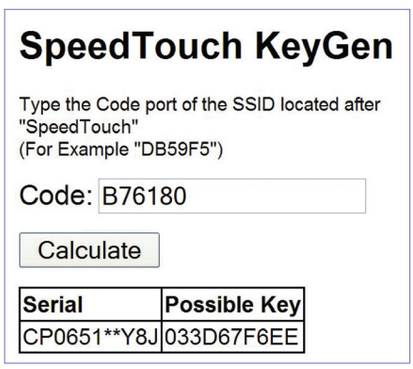
terhalen is. Ook in Spanje en Engeland zijn er meldingen van dit probleem. Het probleem doet zich niet voor bij de zilverkleurige Experiabox (made by Siemens).

Het modem zendt standaard de naam van het draadloze netwerk uit (SSID Broadcast). 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 WPA-codes die verstopt zitten in de laatste zes tekens van de SSID.

Die laatste zes tekens van de door KPN verstrekte SSID is dan met een simpel programmaatje te herleiden tot de WPA-beveiligingscode zoals die (meestal) door de KPN-ADSL-provider bij aflevering aangeleverd is. Als je daarna je WPA-code en/of SSID niet hebt veranderd, kan een kwaadwillende daarmee gemakkelijk toegang tot je internetverbinding (en je computer) krijgen.



De SSID is zichtbaar in de set-up, maar wordt ook voor iedereen zichtbaar uitgezonden.



SpeedTouch Modem KeyGen op www.speedtouch.websijt.net

Je kunt zelf achterhalen of dit voor jou geldt: test de laatste zes tekens van het SSID met het miniprogrammaatje 'speedtouchkey.exe' dat je van internet haalt. Dat kan nog makkelijker door de code van je SSID in te typen op www.speedtouch.websijt.net.

Als jouw WPA-code dan in beeld verschijnt, weet je dat de beveiliging van je draadloos netwerk ondeugdelijk is. Verschijnt de juiste code niet, dan loopt jouw draadloze router dat inbraakrisico in beginsel niet.

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 iemand die kwaad wil deze beveiliging kan omzeilen. En die worden door KPN ook gewoon aangesloten.

KPN raadt aan om de SSID te wijzigen, zodat herleiden van je WPA-code onmogelijk wordt. Een matig advies, je kunt de SSID-naam van je buurman immers al ergens genoteerd 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.

Controleer ook de instellingen van je modem als de KPN daar 'onderhoud' aan heeft uitgevoerd. Er zijn gevallen bekend waarbij de beveiliging door de gebruiker was gewijzigd, maar door de KPN-monteur weer werd teruggezet naar de (onveilige) situatie bij aflevering!

Als je WiFi-netwerk niet of onvoldoende is beveiligd, kunnen derden je 'afluisteren' en via jouw ADSL-verbinding het internet op. Dat is in Nederland illegaal, maar de dader is dan vaak niet meer te vinden. Er zou bijvoorbeeld via jouw aansluiting illegaal materiaal op het internet gezet kunnen worden. En dan heb jij een probleem omdat je niet kunt aantonen dat een ander dat deed.

Dus nogmaals: altijd op z'n minst de SSID en beveiligingssleutel wijzigen. En natuurlijk ook de inlognaam en het wachtwoord om in de set-up van het modem te komen. Niet alleen met KPN-modems, maar altijd!

DOSgg VraagBaak nabij

Heb jij dat ook wel eens, dat je tegen een probleem aanloopt en dat denkt op te lossen door naar het probleem te 'googelen'? En dat je dan soms een aantal 'oplossingen' vindt, 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 een computer kunt tegenkomen.

Op de site is beschreven hoe je contact kunt opnemen. Je kunt mailen of bellen. Heb je haast, dan bel je 0317-707425. Via een keuzemenu wordt je naar de juiste VraagBaak geleid. Kun je even wachten, 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.

Ook kun je van tevoren 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 van tevoren alles wat daarin geplaatst gaat worden. Afgelopen week zat daar een artikel bij van Ruud Uphoff, een VraagBaak van het eerste uur, met een ontzaglijke hoeveelheid praktische kennis.

In dat artikel beschrijft Ruud de oplossing van een twaalftal veel voorkomende problemen. Onder meer hoe je ervoor kunt zorgen 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 precies met dat probleem kampte. Uiteraard kon ik hem toen Ruuds oplossing toesturen. De dag daarna kreeg ik het bericht dat de foute instelling met succes was gerepareerd. Bedankt Ruud!

Rob de Waal Malefijt