Laatste nieuws

Eerdere berichten

Laatste nieuws
- Paneelmodel zoekt de zon op
- Nanoschijven
- Beeldscherm op je arm
- Bacteriën die drijven of geuren
- Namaakbrein
- Nieuwe rage: laat uw machine twitteren
- URL's worden anderstalig
- Meervoudig lichtsignaal
- De slapeloze computer
- Wolframs zoekmachine rekent zelfs in 'inchdollars'

Gerelateerd nieuws
- De landkaart komt tot leven
- Robots zijn autisten
- De droomcomputers komen
- Het raadsel dat Twitter heet
- Iedereen een supercomputer
- Worstelen met een worm
- Terug naar de maan
- De zwart-witte revolutie
- Dokteren op afstand
- De man die het internet voorzag

Hacken voor domme schaapjes

Iedereen kan hacken met de applicatie Firesheep, in Mozilla's Firefox. Met een muisklik kaapt het programma Facebook- en Twitterpagina's, mits de eigenaar van de pagina op een onbeschermd wifi-netwerk surft. Software-ontwerper Eric Butler lanceerde Firesheep eind oktober op een congres voor hackers in San Diego.

Sonny kijkt beduusd als ik hem aanspreek: 'Een vriend belde mij net dat mijn Facebook is gehacked. Dit is wel echt scary.' Het is dus gelukt en het was kinderlijk eenvoudig. Bewapend met een laptop met de Firesheep applicatie was ik op zoek gegaan naar wifi-hotspots, plaatsen waar je samen met een heleboel andere internetters op een openbaar netwerk kunt surfen. Ik belandde in Grand Café de Balie, in Amsterdam.

Na een uur wachten had ik beet: Sonny diende zich aan in mijn Firesheepvenster. Met een klik op zijn foto kon ik uit zijn naam berichten versturen, zijn foto's bekijken en zijn instellingen veranderen. Het moeilijkste van deze expeditie was om Sonny te herkennen tussen de andere internetters in het Grand Café: op veel Facebookfoto's droeg hij een grote zonnebril.

Met Firesheep wil Butler websites dwingen hun gebruikers beter te beschermen. De meeste websites versleutelen volgens hem wel de inloggegevens, maar wanneer die eenmaal zijn goedgekeurd, laten veel websites hun gebruikers volgens Butler in de kou staan.

Als naam en wachtwoord correct zijn ingevoerd, versturen websites als Facebook en Twitter een niet-versleutelde cookie die de browser voor alle volgende activiteiten op de website gebruikt. Op openbare wifi-netwerken, zoals op sommige treinstations en cafés, suizen deze cookies je om de oren, volgens Butler. Firesheep onderschept de cookies en zo kan iedereen Facebook- en Twitterpagina's met een dubbele muisklik hacken.

Puberende familieleden
Het is een bekend probleem dat, volgens wiskundige Benne de Weger, van de technische universiteit Eindhoven, vooral bij de websites zelf ligt. De Weger: 'Sites als Facebook hebben tot nu toe de keuze gemaakt om niet te investeren in het versleutelen van de gegevens van hun leden. De vraag is natuurlijk of dat een bewuste keuze is geweest. Door Firesheep worden ze in ieder geval gedwongen om een bewuste keuze te maken.'

Het versleutelen van de data is in principe niet moeilijk, volgens De Weger, maar er zitten wel nadelen aan. De verbinding wordt er bijvoorbeeld iets langzamer van en het kost meer servercapaciteit. De extra capaciteit kost de website geld. Ook volgens Butler is het niet onmogelijk voor websites om al het internetverkeer op hun site te versleutelen. Zo meldt hij op zijn weblog dat bijvoorbeeld Google's gmail dit sinds kort doet.

Butler benadrukt dat het probleem niet bij het onbeveiligde internet ligt. 'Een wifi-internetverbinding met wachtwoord (WPA2) vereist van de hacker maar één stap extra.' Ook voor deze stap zijn volgens Butler programma's te downloaden die de klus voor je klaren, zoals Cain & Abel. Bovendien kan iedereen die op hetzelfde beveiligde netwerk zit, alsnog inbreken. Een wachtwoord beschermt dus niet tegen Firesheepaanvallen van puberende familieleden of collega's.

Toch hoeven we niet werkeloos toe te zien hoe Firesheepgebruikers of andere hackers op openbare netwerken met onze Facebookpagina's aan de haal gaan. Op internet zijn programma's te vinden die bepaalde sites dwingen hun gegevens te versleutelen, zoals HTTPS Everywhere. De applicatie in Firefox, die in ieder geval kan beschermen tegen Firesheep, heet Force-TLS. Ook voor Google Chrome is een soortgelijke uitbreiding te vinden. Het is wel oppassen geblazen, want deze programma's werken bij lang niet alle websites of alle versies van de internet browsers.

Jet Salomons

Reacties (0)

Er zijn nog geen reacties.

Reageren

Naam:

Email *(Niet verplicht)*: Zichtbaar

Bericht:

Login Zoek

Abonnement

Aanbiedingen

Adverteren

Proefabonnement

Deze maand

NWTweets

NWT
158 followers

Koenjit voor je lever, nieuws http://bit.ly/98x4GL
7 minuten geleden

Willen alle verwijfde mannen opstaan?, weblog http://bit.ly/bA0fs6
ongeveer 19 uur geleden

Hacken voor domme schaapjes, nieuws http://bit.ly/bjkGZa
1 dag geleden

Dikke fruitvlieg model voor zwaargewichten, nieuws http://bit.ly/dl269s
1 dag geleden

Kippenvel voor biologen, weblog http://bit.ly/bPnzoJ
2 dagen geleden