OUCH! | February 2016

Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers.

OUCH!

IN DEZE EDITIE...

- Jouw Draadloos Netwerk
- Jouw Toestellen

Jouw Thuisnetwerk Beveiligen

Overzicht

Enkele jaren geleden was een thuisnetwerk relatief eenvoudig, het bestond simpelweg uit een draadloze access point en één of twee computers die gebruikt werden om te surfen, online te gamen of shopping. Intussen zijn thuisnetwerken complexer geworden. Er zijn meer toestellen bijgekomen die we voor meer gebruiken dan enkel het Internet te browsen of om media te bekijken. In deze nieuwsbrief gaan we in op hoe je thuis een veilig netwerk kan voorzien voor jezelf en jouw familie.

Gast redacteur

Cheryl Conley leidt het Security Education en Awareness team bij Lockheed Martin, met “The I Campaign™” bereikt ze meer dan 100 000 werknemers. Dit omvat gerichte focusgroepen in de onderneming en een globaal antiphishing programma. Volgt Cheryl op Twitter via **@conleychera**.

Jouw Draadloos Netwerk

Bijna ieder thuisnetwerk bestaat uit een draadloos netwerk (ook wel bekend als een Wifi-netwerk). Hiermee kan je een draadloze verbinding maken met het Internet, zowel met je laptop, tablet, spelconsole of televisie. De meeste draadloze thuisnetwerken worden beheerd door jouw Internet router, dit is het toestel dat jouw Internet Service Provider bij jouw thuis heeft geïnstalleerd om je te verbinden met het Internet. Hoewel in sommige gevallen kan jouw draadloos netwerk beheerd worden door een apart systeem, dat bekend staat als een draadloze access point die jouw Internet router verbindt. Ongeacht het soort van draadloos netwerk, worden de draadloze signalen op dezelfde manier uitgezonden. De verschillende toestellen in jouw huis verbinden met het netwerk via deze draadloze signalen. Hiermee kunnen deze toestellen verbinding maken met het Internet net zoals de andere toestellen op jouw thuisnetwerk. Het beveiligen van jouw draadloos netwerk is daarmee het belangrijkste om jouw huis beveiligen. Om dit te doen, raden we volgende stappen aan:

- Verander het standaard admin wachtwoord van jouw Internet router of draadloos access point. De admin login laat je toe om de instellingen van jouw draadloos netwerk te beheren. Het probleem is dat veel Internet routers en draadloze access points een standaard admin login en wachtwoord hebben dat gekend is en zelfs gepubliceerd is op het Internet. Net daarom verander je best het admin wachtwoord in een sterk en uniek wachtwoord dat enkel jij kent.
- Wijzig de standaardnaam van je draadloos netwerk (soms ook de SSID genoemd). Dit is de naam die jouw toestellen zien als ze zoeken naar een lokaal draadloos netwerk. Geef je netwerk een unieke naam zodat je het makkelijk

Jouw Thuisnetwerk Beveiligen

kunt identificeren, maar zorg ervoor dat het geen persoonlijke gegevens bevat. Verberg de naam van je netwerk niet, aangezien aanvallers scanning tools gebruiken die deze verborgen netwerken kunnen tonen.

- Zorg ervoor dat je enkel mensen die je vertrouwt laat verbinden met jouw draadloos netwerk en dat de verbindingen versleuteld zijn. Dit kan je doen door een sterke beveiliging te voorzien. Momenteel biedt WPA2 de beste beveiliging. Als je dit inschakelt, dient men eerst een wachtwoord op te geven vooraleer men kan verbinden met het netwerk. WPA2 versleutelt ook iedere verbinding. Zorg ervoor dat je geen oudere beveiligingsmethoden kiest zoals WEP, die geen beveiliging bieden waardoor je een open netwerk maakt. Bij open netwerken kan iedereen met jouw draadloos netwerk verbinden zonder enige vorm van authenticatie.

Om je thuisnetwerk te beveiligen; beveilig je jouw draadloos netwerk, voorzie je updates en wachtwoorden op al jouw toestellen binnen het netwerk.

- Zorg ervoor dat het wachtwoord waarmee mensen verbinding maken met jouw draadloos netwerk een sterk wachtwoord is dat verschilt van het admin wachtwoord. Onthoud dat je het wachtwoord slechts één keer moet ingeven in elk toestel, vermits ze het wachtwoord kunnen opslaan en onthouden.
- Talloze draadloze netwerken ondersteunen een zogenaamde Guest netwerk. Hierdoor kunnen bezoekers op het Internet, maar is jouw thuisnetwerk gescheiden. Dit betekent dat bezoekers niet kunnen verbinden met de toestellen op jouw thuisnetwerk.
- Schakel WiFi Protected Setup of andere mechanismen uit waarmee een nieuw toestel zich kan verbinden met het netwerk zonder het wachtwoord of andere instellingen te weten.
- Heb je moeite met het onthouden van de verschillende wachtwoorden, dan biedt een password manager hulp voor dit probleem.

Ben je niet zeker hoe je deze stappen kan uitvoeren? Vraag meer info bij jouw Internet Service Provider, lees de handleiding van jouw Internet router of draadloze access point of bezoek de website van de producent.

Jouw Toestellen

De volgende stap is om te weten welke toestellen er verbonden zijn met jouw netwerk en ervoor te zorgen dat deze toestellen veilig zijn. Vroeger was dit eenvoudig aangezien er slechts enkele toestellen verbonden waren. In de huidige

Jouw Thuisnetwerk Beveiligen

"continu verbonden" wereld kan bijna ieder toestel zich verbinden met het thuisnetwerk. TVs, spelconsoles, baby monitors, luidsprekers, jouw thermostaat of zelfs jouw auto… Een eenvoudige manier om te bepalen welke toestellen er allemaal verbonden zijn met jouw netwerk, is door een netwerk scanner te gebruiken als Fing. Deze app, die je kan installeren op een computer of mobiel toestel, scant jouw draadloos netwerk en geeft ieder toestel weer dat ermee verbonden is. Eens je alle toestellen hebt gevonden, zorg je er voor dat deze veilig zijn. De beste manier om dit te doen, is door de laatste versie van het besturingssysteem of firmware te voorzien. Indien mogelijk, schakel dan automatische updates in. Indien er een toestel een wachtwoord vereist, kies dan een uniek en sterk wachtwoord. Ten slotte, raadpleeg de website van jouw Internet Service Provider, want deze kan misschien gratis tools beschikbaar stellen waarmee je jouw thuiswerknetwerk mee kan beveiligen.

Meer Weten?

Ga naar http://www.securingthehuman.org om je te abonneren op de maandelijkse OUCH! Security awareness nieuwsbrief, toegang te krijgen tot het OUCH! archief en kom meer te weten over SANS security awareness oplossingen.

Over Cegeka Groep

Cegeka Groep is een onafhankelijke ICT-dienstverlener opgericht in 1992. Cegeka heeft zijn hoofdkantoor in België en heeft vestigingen in België, Duitsland, Frankrijk, Italië, Nederland, Luxemburg, Oostenrijk, Polen, Roemenië, Tsjechië en Slovakije. Het bedrijf levert diensten aan klanten in heel Europa: enterprise cloud- en securitydiensten, applicatiediensten, agile coaching en outsourcingdiensten. Cegeka stelt 3.200 mensen tewerk en haalde in 2013 een omzet van 330 miljoen euro. Bezoek www.cegeka.com voor meer informatie.

Bronnen (Engels)

Passphrases:	https://securingthehuman.sans.org/ouch/2015#april2015
Password Manager:	https://securingthehuman.sans.org/ouch/2015#october2015
Securing Your New Tablet:	https://securingthehuman.sans.org/ouch/2016#january2016
Mapping Your Home Network:	http://l.rud.is/home-network-mapping
Wifi Thuis:	https://veiliginternetten.nl/themes/draadloos-internet/wifi-thuis/

Redactie: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Vertaald door: Sven Jacobs, Tom Palmaers