OUCH! | Januari 2014

De Maandelijkse Beveiligingsnieuwsbrief voor Computergebruikers

OUCH!

IN DEZE EDITIE...

- Draadloos netwerk
- OpenDNS
- Apparaten

Beveilig je Thuisnetwerk

Inleiding

Tot enkele jaren geleden waren thuisnetwerken relatief eenvoudig van opzet, gewoonlijk een draadloze router en misschien een paar computers om te surfen of online te gamen. Thuisnetwerken zijn echter steeds complexer geworden. We gebruiken niet alleen meer apparaten, maar gebruiken ze ook voor meer uiteenlopende zaken. In deze editie behandelen we een aantal eenvoudige maatregelen die je kan nemen om je thuisnetwerk beter te beveiligen.

Auteur

Kevin Johnson is CEO van Secure Ideas, leidt **MySecurityScanner.com** n is een senior instructor van het SANS Institute. Je kan meer informatie vinden op **www.secureideas.com**.

Draadloos netwerk

Vrijwel ieder thuisnetwerk beschikt over een draadloos-, of WiFi netwerk. Dit zorgt ervoor dat alle apparaten draadloos met het Internet kunnen verbinden; van laptops en tablets, tot spelcomputers en televisies. Hiervoor maakt het netwerk gebruik van een accesspoint. Dit apparaat heeft een vaste verbinding met de Internet router en is tegenwoordig vaak zelfs standaard in de Internet router ingebouwd. Deze radio zender zendt het draadloze signaal uit waarmee alle apparaten verbinden om toegang te krijgen tot het thuisnetwerk. Eenmaal verbonden kunnen alle apparaten communiceren met het Internet, maar ook met elkaar. Dit maakt het draadloze accesspoint of router tot één van de belangrijkste onderdelen van het thuisnetwerk. Gebruik de volgende tips om je thuisnetwerk beter te beveiligen.

- Standaard wachtwoorden van de meeste routers en accesspoint en routers zijn gewoon op het Internet te vinden. Verander dus het standaard administrator wachtwoord. Zorg dat het uniek is en gebruik het niet voor andere accounts.
- Een andere optie die je kan wijzigen is de netwerk naam of SSID. Verander het in iets dat je eenvoudig kan identificeren, maar zorg dat het geen persoonlijke informatie bevat. Je hebt vaak de mogelijkheid om het SSID te verbergen (hide SSID of non-broadcast) maar dit een vrij nutteloze optie aangezien de meeste scanners hier eenvoudig omheen gaan.

Beveilig je Thuisnetwerk

- Vervolgens moet je er voor zorgen dat uitsluitend mensen die je vertrouwt toegang krijgen tot je netwerk en dat de verbindingen versleuteld zijn. Op dit moment kan je daar het beste WPA2 voor gebruiken. Door dit aan te zetten in de router zorg je ervoor dat iedereen zich met een wachtwoord moet aanmelden op je netwerk en worden de verbindingen automatisch versleuteld. Gebruik in geen geval WEP of een Open network; WEP is oud en bijzonder eenvoudig te kraken en met een Open network zorg je iedereen met je netwerk kan verbinden.
- Maak het verbindingswachtwoord lang en moeilijk te raden en gebruik vooral niet hetzelfde wachtwoord je als administrator wachtwoord hebt ingesteld. Je hoeft het immers maar één keer op je apparaten in te voeren en vervolgens onthouden ze het gewoon.
- Veel routers en accesspoints hebben een 'guest network' of gasten netwerk functie. Via dit netwerk kunnen bezoekers wel naar het Internet, maar niet verbinden met andere apparaten. Zorg dat je ook hier WPA2 configureert en gebruikt uiteraard ook hier weer een ander wachtwoord.
- Indien het wat te veel wachtwoorden zijn om te onthouden, gebruik dan een password manager om ze veilig op te slaan.

Gebruik WPA2 om je draadloze thuisnetwerk te beveiligen, overweeg een dienst als OpenDNS en zorg dat al je apparaten up-to-date zijn.

OpenDNS

Wanneer je klaar bent met het instellen van het draadloze netwerk, kan je overwegen om je thuisnetwerk met OpenDNS te configureren (of een vergelijkbare dienst als Norton ConnectSafe for Home). Wanneer je een website opent dan zorgt DNS ervoor dat je computer weet met welke Internet server hij moet verbinden. Diensten als OpenDNS houden een lijst bij van bekende, geïnfecteerde websites en zorgen ervoor dat apparaten daar niet mee kunnen verbinden. Tevens heb je de mogelijkheid om bepaalde soorten Internet sites te blokkeren (downloads, geweld, seks, etc.). Wat OpenDNS zo handig maakt, is dat je niet op al je apparaten een apart programmaatje hoeft te installeren. Je hoeft alleen de DNS instellingen op de Internet router maar aan te passen en je bent klaar.

Beveilig je Thuisnetwerk

Apparaten

Vervolgens is het goed om te weten welke apparaten er allemaal verbinden met je netwerk en of ze beveiligd zijn. Dit was vroeger een stuk eenvoudiger aangezien er maar een paar apparaten verbonden waren. Tegenwoordig echter, kan bijna alles verbinden met een netwerk. Bijvoorbeeld TV's, spelcomputers, babyfoons, luidsprekers, versterkers, thermostaten en soms zelfs auto's. De eenvoudigste manier om al deze apparaten veilig te houden is te zorgen dat de laatste software versies en updates geïnstalleerd zijn. Maak, indien mogelijk, gebruik van de auto-update functie en kijk anders iedere maand even op de website van de fabrikant of er updates zijn. Verder bieden Internet Service Providers (ISP) tegenwoordig vaak ook gratis tools of diensten die je kunnen helpen je thuisnetwerk te beveiligen.

Meer Weten?

Ga naar http://www.securingthehuman.org om je in te schrijven voor de maandelijkse OUCH! nieuwsbrief, toegang tot het OUCH! archief en om meer te weten te komen over SANS Security Awareness programma's.

Nederlandse Editie

De Nederlandse editie van OUCH! wordt gesponsord door Breukel IIS. Wij brengen enterprise information security naar het midden- en klein bedrijf. Voor meer informatie: info@breukeliis.com

Bronnen (Engels)

OpenDNS:
http://www.opendns.org
Norton ConnectSafe:
http://dns.norton.com/dnsweb/dnsForHome.do
Network Security Scanner:
http://www.sophos.com/en-us/products/free-tools/network-security-scan.aspx
Password Managers:
http://www.securingthehuman.org/resources/newsletters/ouch/2013#october2013

Redactie: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Vertaald door: Jan-Adam Breukel