Bilgisayar Kullanıcıları için Aylık Güvenlik Farkındalığı Bülteni

OUCH!

BU SAYIDA...

Ev Ağınızı Güvenli Hale Getirmek

Genel Bakış

Birkaç yıl önce ev ağları göreceli olarak daha basitti, hatta genellikle bir kablosuz ağ noktası ve internette gezmek veya oyun oynamak, alışveriş yapmak için kullanılan bir ya da iki bilgisayardan oluşuyordu. Ancak ev ağları giderek karmaşıklaşıyor. Artık ev ağımızda çok fazla sayıda cihazımız var ve sadece internette gezmek ve birşeyler izlemek için kullanmıyoruz. Bu bültenimizde kendiniz ve aileniz için nasıl bir güvenli ev ağı oluşturabileceğinizi değerlendireceğiz.

Konuk Yazar

Cheryl Conley, Lockheed Martin'de 100.000'den fazla çalışana ulaşan "Ben (The "I" ™)" kampanyasının ve Güvenlik Eğitimi ve Farkındalığı ekibinin yöneticisidir. Bu kampanya oltama saldırıları ile mücadele eden kurum çapındaki odak grupların birlikteliği ve savunuculuğunu da kapsıyor. Cheryl'i **@conleychera** hesabından takip edebilirsiniz.

Kablosuz Ağınız

Hemen hemen her ev ağı bir kablosuz ağ (Wi-Fi ağ) ile başlar. Bu ağ, sizin bilgisayarlarınız, tabletleriniz, oyun konsollarınız, televizyonlarınız gibi herhangi bir cihazınızdan internete kablosuz olarak bağlanmanızı sağlar. Birçok ev kablosuz ağı, internet servis sağlayıcınız tarafından evinize kurulan internet yönlendirici cihaz tarafından kontrol edilir. Ancak bazı durumlarda kablosuz ağınız internet yönlendiricinize bağlanan ayrı bir kablosuz erişim noktası tarafından da kontrol edilebilir. Hangi şekilde kontrol edildiğinden bağımsız olarak, ikisi de kablosuz sinyalleri yayımlayarak çalışır. Evinizdeki değişik cihazlar da bu sinyalleri kullanarak kablosuz ağınıza bağlanırlar. Buradan, bu cihazlar ev ağınızdaki diğer cihazlar gibi internete bağlanabilirler. Bu da, kablosuz ev ağınızı güvenli hale getirmenin evinizi korumanın önemli bir parçası olduğu anlamına gelir. Güvenli hale getirmeniz için aşağıdaki adımları izlemenizi öneriyoruz:

- Internet yönlendiriciniz ya da kablosuz erişim noktanızı varsayılan yönetici hesabının (administrator) parolalarını değiştirin. Yönetici hesapları, kablosuz ağ ayarlarını yapmanızı sağlayan yetkili bir hesaptır. Birçok Internet yönlendirici ya da kablosuz erişim noktası herkes tarafından bilinen, internette bulunabilen yönetici hesap isimleri ve parolaları ile konfigure edilmiş bir şekilde satılır. Değiştirdiğiniz parolaların sadece sizin bildiğiniz ve güçlü, tekil parolalar olduğundan emin olun.
- Kablosuz ağınızın (SSID) varsayılan adını değiştirin. Bu, yerel kablosuz ağ taraması yapıldığında cihazlarınızın gördüğü isimdir. Ağınıza kendinizin hemen tanıyabileceği tekil bir isim verin, ancak bunu yaparken kişisel bir bilgi içermediğinden emin olun. Ağınızı gizli/yayın yapmayan modda konfigüre edebilirsiniz ancak birçok tarama aracı ve yetenekli kötü niyetli kişiler bu ağları kolaylıkla keşfedebilirler.

Ev Ağınızı Güvenli Hale Getirmek

- Sadece güvendiğiniz kişilerin kablosuz ev ağınıza bağlandığından ve iletişimin şifrelenmiş şekilde yapıldığından emin olun. Bunu güçlü güvenlik parametrelerini açarak yapabilirsiniz. Şu an için en iyi seçenek WPA2 mekanizmasını kullanmak. Bu parametreyi seçtiğinizde ev ağınıza bağlanmak isteyenlere parola sorulacak ve bağlandıklarında tüm çevrimiçi işlemleri şifrelenmiş olarak gerçekleştirilecek. WEP ya da güvenlik parametresini seçmeyerek (açık ağ anlamına gelecektir) kullanmadığınızdan emin olun. Açık bir ağ, herhangi bir yetkilendirme olmaksızın herkesin kablosuz ağınıza bağlanabileceği anlamına gelir.
- Kablosuz ağa bağlanmak için kullandığınız parolanın güçlü bir parola olduğundan ve yönetici parolasından farklı olduğundan emin olun. Büyük olasılıkla cihazlarınızın her biri için sadece bir kez parolanızı girmeniz gerektiğini, cihazların bu parolayı üzerlerinde sakladığını hatırlayın.

Ev ağınızı korumak için; kablosuz ağınızı güvenli hale getirin ve ağınızdaki tüm cihazları güncel tutun ve parola ile koruyun.

- Birçok kablosuz ağ “Misafir Ağı”nı desteklemektedir. Bu ziyaretçilerinizin internete bağlanması için izin verir, ancak ev ağınızdaki diğer cihazların herhangi bağlanmalarını engelleyerek ev ağınızı korur. Bir misafir ağı eklerseniz, bu ağ için de benzersiz bir parola ve WPA2 parametresini etkinleştirdiğinizden emin olun.
- WiFi Korumalı Ayar (WiFi Protected Setup) veya parola ve yapılandırma seçeneklerini bilmeden yeni bir cihazı ağa bağlanmak için izin veren diğer mekanizmaları engelleyin.
- Eğer tüm bu farklı parolaları hatırlamakta zorluk yaşıyorsanız sizin için bunları saklayacak bir parola yöneticisi kullanmanızı öneririz.

Tüm bu adımları nasıl uygulayacağınızdan emin değil misiniz ? Internet Hizmet Sağlayıcınıza danışın, internet yönlendiriciniz ya da kablosuz erişim noktanızın cihaz dokümantasyonuna ya da internet sitelerindeki bilgilere bakın.

Cihazlarınız

Bir sonraki adım, ev ağınıza nelerin bağlı olduğunu bilmeniz ve bu cihazların tümünün güvenli olduğundan emin olmanız. Bu durum bağlı sadece birkaç cihazının olduğu durumda çok kolaydır. Ancak bugünün “her zaman bağlı” dünyasında neredeyse herşeyiniz, TV’leriniz, oyun konsollarınız, bebek monitörleriniz, hoparlörleriniz, termostatınız hatta belki arabanız da dahil olmak üzere ev ağınıza bağlısınız / bağlanabilirsiniz. Ev ağınızda nelerin bağlı olduğunu keşfetmek için Fing gibi basit bir ağ tarayıcı

Ev Ağınızı Güvenli Hale Getirmek

kullanabilirsiniz. Bilgisayarınıza veya mobil cihazınıza yükleyebileceğiniz bu tarz uygulamalar, kablosuz ağınızı tarar ve bağlı her cihazı raporlar. Ev ağınızdaki tüm cihazları tespit ettikten sonra, cihazların her birinin güvenli olduğundan emin olmanız gerekir. Bunu yapmanın en iyi yolu cihazlarınızın işletim sistemi / firmware sürümlerinin her zaman en son sürümde olmasını sağlamaktır. Mümkün oldukça, cihazlarınızda otomatik güncelleştirme seçeneklerini etkinleştirin. Cihazlarınız için herhangi bir parola gerekiyorsa, her zaman benzersiz ve güçlü bir parola kullanın. Son olarak, ev ağınızı güvenli hale getirmek için ücretsiz araçlar sağlayabilecek olan internet servis sağlayıcınızın web sitesini ziyaret ettiğinizden emin olun.

Daha Fazla Bilgi İçin

Aylık OUCH! güvenlik farkındalığı bültenine üye olun, OUCH! arşivlerine erişin ve http://www.securingthehuman.org adresini ziyaret ederek SANS güvenlik farkındalığı çözümleri hakkında daha fazla bilgi edinin.

Türkçe Çevirisi

Selma Süloğlu, ODTÜ Bilgisayar Mühendisliğinde doktorasını tamamlamış olup SOSoft Bilişim Teknolojilerinde biyometrik güvenlik sistemleri üzerinde çalışmaktadır.

Sema Yüce, Türkiye'nin önde gelen kurumsal şirketlerinde ve özellikle bilişim, telekomünikasyon, sanayi, perakendecilik gibi sektörlerde; bilgi güvenliği, iş sürekliliği, risk yönetimi, altyapı hizmetleri, yazılım geliştirme ve proje yönetimi alanlarında yönetici ve danışman olarak 15 yılı aşkın süredir görev yapmaktadır.

Kaynaklar

Parolalar:	https://securingthehuman.sans.org/ouch/2015#april2015
Parola Yöneticileri:	https://securingthehuman.sans.org/ouch/2015#october2015
Yeni Tabletinizi Güvenli Hale Getirmek:	https://securingthehuman.sans.org/ouch/2016#january2016
Ev Ağınızı Haritalandırmak:	http://l.rud.is/home-network-mapping

Yayın Kurulu : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis