Bilgisayar Kullanıcıları için Aylık Güvenlik Farkındalığı Bülteni

OUCH!

BU SAYIDA...

Ev Ağınızı Güvenli Hale Getirmek

Özet

Birkaç yıl önce ev ağları göreceli olarak daha basitti, muhtemelen ev ağınız bir kablosuz erişim noktası ve internette gezmek ya da online oyun oynamak için kullanılan bir ya da iki bilgisayardan oluşuyordu. Ancak ev ağları giderek karmaşıklaşıyor. Bunun nedeni sadece bağlandığımız cihaz sayısının artması değil, ev ağlarını kullanarak yaptığımız işlerin artması. Bu sayıda daha güvenli bir ev ağı oluşturmak için gereken temel adımları değerlendiriyor olacağız.

Konuk Editör

Kevin Johnson Secure Ideas'da CEO, **MySecurityScanner.com** yürütücüsü ve SANS Enstitüsü'nde kıdemli eğitmendir. Daha fazla bilgi için **www.secureideas.com** adresini kullanabilirsiniz.

Kablosuz Ağınız

Neredeyse her ev ağı, bir kablosuz ağ (bazen Wi-Fi ağ diye de nitelendirilir) ile başlar. Bu, sizin dizüstü bilgisayarlarınızdan tabletlerinize ya da oyun konsolu ve televizyonlarınıza kadar herhangi bir cihazınızı internete bağlamanızı sağlayan şeydir. Bunun olabilmesi için kablosuz ağınız, "kablosuz erişim noktası"na ihtiyaç duyar. Bu da, Internet yönlendiricinize bağlanan (ya da içinde olan) bir fiziksel araçtır ve bağlanan cihazlarınıza kablosuz sinyaller gönderir. Cihazlarınız bir kez erişim noktasına bağlandığında internete bağlanabildiği gibi, ev ağınıza bağlı diğer cihazlara da bağlanabilir. Sonuç olarak, kablosuz erişim noktanız, ev ağınızın kritik bileşenlerinden biridir ve aşağıdaki adımlarla korumanızı öneririz.

- Kablosuz erişim noktalarının birçoğu için varsayılan yönetici adı ve şifre herkes tarafından bilinen ve hatta sık sık internette yayınlanan bilgilerdir. Bu nedenle, varsayılan yönetici adı ve şifresini sadece sizin bildiğiniz şeylerle değiştirdiğinizden emin olun. Bu benzersiz parola olsun ve başka herhangi bir hesabınızda kullanmayın.
- Diğer bir seçenek ev ağınızın ismini (SSID olarak da bilinir) özelleştirmektir. Bu, sizin cihazlarınızın yerel kablosuz ağları ararken göreceği isimdir. Ağınıza kolaylıkla diğerlerinden ayrıştırabileceğiniz ancak herhangi bir kişisel bilgi taşımayan bir benzersiz isim verin. Aynı zamanda ağınızı gizli (ya da yayın yapmayan) şekilde konfigüre etmekte de az da olsa yarar var. Çoğu kablosuz ağ tarama aracı ya da yetenekli bir saldırgan kolaylıkla gizli bir ağın detaylarını açığa çıkarabilir.

Ev Ağınızı Güvenli Hale Getirmek

- Bir sonraki adım, sadece sizin bildiğiniz ve güvendiğiniz insanların bağlanabilmesi ve kablosuz ağınızı kullanması ve bu bağlantılarında şifreli olmasını sağlama adımıdır. Komşularınız ya da yabancıların bağlanamadığı veya ağınızı izleyemediğinden emin olun. Bu riskleri kolaylıkla kablosuz erişim noktası üzerinde güçlü bir güvenlik sağlayarak azaltabilirsiniz. Şu anda en iyi seçenek güvenlik mekanizması olarak WPA2 kullanmaktır. Sadece bunu etkinleştirmek ev ağınıza bağlanacak insanlar için bir parola girişini gerektirir ve bir kez doğrulandıktan sonra bu bağlantılar şifrelenir. Eski, güncel olmayan güvenlik yöntemleri (örneğin WEP) kullanan ya da hiç güvenlik kullanmayan (açık ağ) yöntemler kullanmadığınızdan emin olun. Açık ağ herhangi bir kimsenin, kimlik doğrulaması olmadan kablosuz ağınıza bağlanmasını sağlar.

Ev ağınızı korumak için, güvenli bir kablosuz ağa sahip olduğunuzdan, OpenDNS ya da benzeri bir servis kullandığınızdan ve ev ağınızdaki bütün cihazların güncellendiğinden ve son sürümlerinin kullanıldığından emin olun.

- Kablosuz ağınıza bağlanan insanların kullandığı parolaların güçlü, tahmin edilmesi zor ve yönetici parolalarından farklı olduğundan emin olun. Parolalarınızı her bir cihazınız için sadece bir kez gireceğinizi ve sonrasında bu parolayı onların saklayacağını unutmayın.
- Birçok kablosuz erişim noktası “Misafir Ağı (Guest Network)”nı destekler. Bir misafir ağı misafirlerinizin kablosuz erişim noktanıza bağlanarak internere erişmelerini sağlar, ancak sizin ev ağınızdaki diğer cihazlara bağlanamazlar. Eğer misafir ağı kullanacaksanız, WPA2 seçeneğini ve bu ağ için farklı bir parolayı kullandığınızdan emin olun.
- Eğer farklı parolaları hatırlamakta zorlanıyorsanız, onları güvenli bir şekilde saklamak için parola yöneticilerini kullanın.

OpenDNS

Kablosuz ağınızı bir kez konfigüre ettikten sonra, ev ağınızı Alan Adı Hizmeti (DNS) sunucusu olarak OpenDNS (ya da Norton ConnectSafe for Home gibi benzer bir servis) kullanacak şekilde ayarlamanızı öneririz. İnternet tarayıcınıza bir isim yazdığınızda, internetteki hangi sunucuya bağlanacağını bulan servis, Alan Adı Hizmeti (DNS) olarak adlandırılır. OpenDNS gibi servisler bilinen, kötü niyetli kodların bulaştığı internet sitelerini belirler ve kablosuz ev ağınızdaki herhangi bir cihazın yanlışlıkla bu internet sitelerini ziyaret etmesini engeller. Ayrıca bu servislerin çoğu size sakıncalı internet sitelerini filtreleme ve kısıtlama seçenekleri de sunar. Bu yaklaşımı bu kadar etkin kılan şey, cihazlarınız üzerine herhangi bir yazılım kurmanıza gerek kalmamasıdır, siz değişikliği sadece kablosuz erişim noktası üzerinde yapıyor olacaksınız.

Ev Ağınızı Güvenli Hale Getirmek

Cihazlarınız

Sonraki adım, ev ağınıza hangi cihazların bağlandığını bilmek ve bu cihazların güvenli olduğundan emin olmaktır. Bu genelde kolaydı, çünkü bağlanan sadece birkaç cihazdı. Ancak bugünlerde televizyonlar, oyun konsolları, bebek izleme cihazları, hoparlörler, evinizin termometresi, hatta arabanız bile ev ağınıza bağlanabiliyor. Ev ağınıza bağlanan cihazları belirlediğinizde ne kadar fazla cihazınız olduğuna şaşırabilirsiniz. Tüm bu cihazları güvenli tutmanın en basit yolu, işletim sistemlerinin her zaman güncel olduğundan emin olmaktır. Mümkün olan durumlar için otomatik güncelleme seçeneğini aktif hale getirin. Eğer mümkün değilse, izleyin ve her ay güncelleyin. Ayrıca, internet servis sağlayıcınızın internet sitesini ziyaret edin, ev ağınızı güvenli hale getirmenize yardım edecek ücretsiz araçlar ve servisler sunabilirler.

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

OpenDNS:
http://www.opendns.org
Norton ConnectSafe:
http://dns.norton.com/dnsweb/dnsForHome.do
Ağ Güvenliği Tarayıcısı:
http://www.sophos.com/en-us/products/free-tools/network-security-scan.aspx
Şifre Yöneticileri:
http://www.securingthehuman.org/resources/newsletters/ouch/2013#october2013

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