Bilgisayar Kullanıcıları için Aylık Güvenlik Farkındalığı Bülteni

OUCH!

BU SAYIDA...

Güvende Olmak için 5 Adım

Giriş

Teknoloji hayatımızda giderek daha fazla önem kazandıkça karmaşıklığı da artmakta. Teknolojinin ne kadar hızlı değiştiği göz önüne alındığında güvenlik önerileriyle başa çıkmak da kafa karıştırıcı olabiliyor. Sanki her zaman ne yapıp ne yapmayacağınızla ilgili yeni bir öğüt olacakmış gibi görünüyor. Ancak nasıl güvende olacağınız hakkında detaylar zamanla değişse bile kendinizi korumak için her zaman yapabileceğiniz temel şeyler var. Kullandığınız teknolojiden ya da kullanım yerinizden bağımsız olarak size aşağıdaki beş kilit adımı öneriyoruz.

Konuk Yazar

Lenny Zeltser, NCR Corp'da müşterilerinin BT operasyonlarının korunması üzerine yoğunlaşmış olup SANS Enstitüsünde kötü amaçlı yazılımlar ile mücadele dersi vermektedir. Lenny'i Twitter'da **@lennyzeltser** ve yazdığı **blog.zeltser.com** güvenlik ağ günlüğünden takip edebilirsiniz.

Beş Kilit Adım

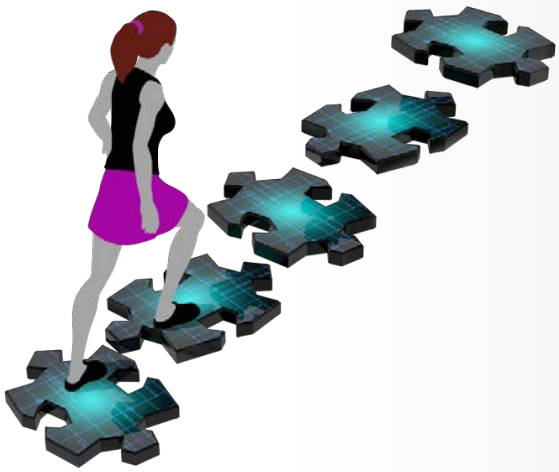
Aşağıdaki beş adımın her biri, basit bir genel bakış verir. Her adım ile ilgili daha fazla bilgi sahibi olmak için bültenin sonundaki Kaynaklar başlığının altına başvurabilirsiniz.

1. **Siz**: Başta ve öncelikle bilmelisiniz ki tek başına teknoloji sizi koruyamaz. Saldırganlar güvenlik teknolojilerinin çoğunu atlatmanın en kolay yolunun size saldırmak olduğunu öğrendiler. Eğer sizin şifrenizi ya da kredi kartı bilgilerinizi istiyorlarsa onlar için bunun en kolay yolu sizi oyuna getirerek bu bilgileri sizden almaktır. Örneğin, sizi Microsoft teknik hizmet personeli gibiymiş gibi arayabilir ve bilgisayarınıza virus bulaştığını öne sürebilirler ki gerçekte bu kişiler siber suçlular olup istedikleri, bilgisayarınıza erişmek için gerekli bilgileri edinmektir. Ya da belki de size paketinizin teslim edilemediğine dair bir e-posta atacaklar ve adresinizi teyit etmek için bir bağlantıyı takip etmenizi isteyeceklerdir ki gerçekte sizin kötü niyetli bir ağ sitesini ziyaret etmenizi sağlayarak bilgisayarınıza izinsiz bir şekilde gireceklerdir. Sonuçta saldırganlara karşı en büyük savunmanız kendinizsiniz. Şüpheci olun, sağduyunuzu kullanarak birçok saldırıyı fark edebilir ve durdurabilirsiniz.

2. **Güncelleme**: Bilgisayarınızın, mobil cihazlarınızın, uygulamalarınızın ve ağınıza bağlı herşeyin üzerinde son versiyon yazılımların kurulu olduğundan ve çalıştığından emin olun. Siber suçlular sürekli olarak kullandığınız teknolojilerin zayıf noktalarını bulmaya çalışırlar. Bir zafiyet yakaladıklarında bu zayıf noktaları kullanarak hangi teknolojiyi kullanıyorsanız ona izinsiz girmeye çalışırlar; ağınız, bilgisayarınız ve mobil cihazlarınız dahil. Eş zamanlı olarak sizin kullandığınız teknolojiyi geliştiren şirketler de yazılımları güncel tutmak için sıkı çalışırlar. Bir zayıf nokta ortaya çıktığında, bu zayıf noktayı onarmak

Güvende Olmak için 5 Adım

için bir yama ortaya çıkarır ve genel kullanım için yayınlarlar. Siz ise bilgisayar ve mobil cihazlarınızın bu güncellemeleri yaptığından emin olarak, bilinen zayıf noktaları azaltıp izinsiz girişleri daha zor hale getirirsiniz. Güncel kalmak için her fırsatta otomatik güncellemeyi etkinleştirin. Bu kural ağa bağlı herhangi bir teknoloji için geçerlidir; internete bağlı televizyonlar, bebek monitörleri, ana yönlendiriciler (home router), oyun konsolları ya da belki bir gün arabanız. Eğer bilgisayarınızın işletim sistemi, mobil cihazınız ya da kullandığınız başka herhangi bir teknoloji artık desteklenmiyor ve artık herhangi bir güncelleme almayacak ise desteklenen yeni bir sürüme geçmenizi öneriyoruz.



Bu beş kilit adımı izleyerek, güncel teknolojileri kullanırken kendinizi korumak adına önemli bir yol almış olacaksınız.

3. **Parolalar**: Kendinizi korumak için bir sonraki adım, her bir cihazınız, çevrim-içi hesabınız ve uygulamalarınız için güçlü ve eşsiz parolalar kullanmayı gerektirir. Buradaki anahtar kelimeler güçlü ve eşsiz'dir. Güçlü bir parola, bilgisayar korsanları ya da onların otomatik araçları tarafından kolayca tahmin edilemeyecek olan bir parola demektir. Yalnız bir kelime yerine sembol ve rakamları ek olarak içeren birden fazla kelimeden oluşan uzun bir parola kullanın. Eşsiz ise her bir cihazınız ve çevrim-içi hesabınız için ayrı bir parola kullanmanız demektir. Bu yolla eğer bir parolanız ele geçirilirse, diğer hesaplarınız ve cihazlarınız hala güvende olacaktır. Güçlü ve eşsiz parolalarınızı hatırlayamıyor musunuz? Üzülmeyin biz de hatırlayamıyoruz. İşte bu yüzden size, tüm parolalarınızı şifreli bir formatta güvenli bir şekilde saklayan, bilgisayarınız ya da mobil cihazınız için özel bir yazılım olan parola yöneticilerini tavsiye ediyoruz. Son olarak eğer hesaplarınızdan herhangi biri iki aşamalı doğrulamayı destekliyorsa her zaman bu özelliği etkinleştirmenizi tavsiye ediyoruz çünkü bu hesabınızı korumanın en güçlü yollarından biridir.

4. **Şifreleme**: Size tavsiye edeceğimiz üçüncü adım şifrelemeyi kullanmaktır. Şifreleme, sadece siz ya da sizin güvenebileceğiniz kişilerin bilgilerinize ulaştığından emin olmanızı sağlar. Veri iki yerde şifrelenir: hareketsiz ya da hareketli iken. Hareketsiz iken verilerin şifrelenmesi, verilerin dosya olarak sabit diskinizde ya da USB çubuğunuzda saklanıyor iken korunması anlamına gelir. Bir çok işletim sistemi, Tüm Disk Şifreleme (TDŞ, Full Disk Encryption) gibi özellikleri kullanarak bütün verilerinizi otomatik olarak sifrelemenize olanak verir. Her fırsatta bunu etkinleştirmenizi öneririz. Hareketli veriyi şifrelemek ise verinizin bilgisayarınızdan ya da cihazınızdan diğer cihazlara aktarılması sırasında şifrelenmesi anlamına gelir; örneğin çevrim-içi bankacılık işlemleri yaparken. Doğrulama yapmanın en kolay yolu, şifreleme etkin ise ziyaret ettiğiniz ağ sitesinin adresinin "https" ile başladığından ve kapalı asma kilit imgesinin adresin yanında bulunduğundan emin olmaktır.

Güvende Olmak için 5 Adım

5. **Yedekleme**: Bazen ne kadar da dikkatli olursanız olun, cihazlarınız ya da hesaplarınızdan biri ele geçebilir. Eğer durum buysa genellikle tek seçenek, bilgisayarınızın ya da mobil cihazınızın kötü amaçlı yazılımlardan arındığından emin olduktan sonra baştan yapılandırmaktır. Saldırgan kişisel dosyalara, resimlere ve diğer bilgilerinize ulaşımınızı engellemiş bile olabilir. Sizin tek seçeneğiniz ise yedeklemelerinizi kullanarak tüm kişisel bilgilerinizi geri yüklemek olabilir. Düzenli olarak önemli bilgilerinizin yedeklemelerini yaptığınızdan emin olun ve bu bilgilerin geri yüklenebilieceğini doğrulayın. Birçok işletim sistemi ve mobil cihaz otomatik yedeklemeyi desteklemektedir.

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

E-posta Oltalama Saldırıları:	http://www.securingthehuman.org/ouch/2013#february2013
Taletinizi Güvenli Tutmak:	http://www.securingthehuman.org/ouch/2013#december2013
Güçlü Parolalar:	http://www.securingthehuman.org/ouch/2013#may2013
Parola Yöneticileri:	http://www.securingthehuman.org/ouch/2013#october2013
İki Aşamalı Doğrulama:	http://www.securingthehuman.org/ouch/2013#august2013
Şifreleme:	http://www.securingthehuman.org/ouch/2014#august2014
Yedekleme:	http://www.securingthehuman.org/ouch/2013#september2013

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