Herkes İçin Aylık Güvenlik Farkındalığı Bülteni

OUCH!

BU SAYIDA...

- Siz
- Parolalar
- Güncelleme
- Yedekleme

Güvende Olmak İçin 4 Adım

Giriş

Teknoloji hayatımızda giderek daha fazla önem kazandıkça karmaşıklığı da artıyor. Teknolojinin ne kadar hızlı değiştiğl 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 uygulayabileceğiniz temel kurallar var. Kullandığınız teknolojiden ya da kullanım yerinden bağımsız olarak size aşağıdaki dört kilit adımı öneriyoruz. Aşağıdaki adımlar hakkında daha detaylı bilgi için, bültenin sonundaki "Kaynaklar" bölümüne bakabilirsiniz.

Konuk Yazar

Ryan Johnson kurumların kaçınılmaz veri sızıntısı olaylarına yanıt vermeye hazırlıklı olmalarını sağlamaya odaklanmıştır ve SANS Enstitüsü'nde Advanced Network Forensics dersleri vermektedir. Ryan'ı Twitter'da **@ForensicRJ** hesabından takip edebilirsiniz.

1. **Siz**: Başta ve öncelikle bilmelisiniz ki teknoloji tek başına sizi tamamen koruyamaz. Saldırganlar en ileri güvenlik teknolojilerinin çoğunu atlatmanın en kolay yolunun size saldırmak olduğunu öğrendiler. Eğer sizin şifrenizi, kredi kartı ya da kişisel bilgilerinizi istiyorlarsa, onlar için bunun en kolay yolu sizi kandırarak 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 gönderecekler ve adresinizi teyit etmek için bir bağlantıyı takip etmenizi isteyeceklerdir ki gerçekte sizin kötü niyetli bir siteyi ziyaret etmenizi sağlayarak bilgisayarınıza izinsiz bir şekilde gireceklerdir. Fidyeci Yazılımlar (Ransomware) ya da CEO Dolandırıcılığı da böyle başlar. Sonuçta saldırganlara karşı en büyük savunmanız kendinizsiniz. Şüpheci olun. Sağduyunuzu kullanarak birçok saldırıyı fark edebilir ve durdurabilirsiniz.

2. **Parolalar**: Kendinizi korumak için bir sonraki adım, herbir cihazınız ve çevrim-içi hesabınız 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. Hatırlaması ve yazması çok zor olan güçlü parolalardan sıkıldınız mı ? Bunların yerine tam cümlelerden oluşan uzun parolaları ("passphrase") kullanmayı deneyin. Tek bir kelime yerine hatırlaması kolay kelime serilerinden oluşan (örneğin "Benim kahvem nerede?") parolalar

Güvende Olmak İçin 4 Adım

kullanın. Ne kadar uzunsa, o kadar güçlü olacaktır. Eşsiz parola 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.

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

Son olarak eğer hesaplarınızdan herhangi biri iki adımlı doğrulamayı (2FA) destekliyorsa her zaman bu özelliği etkinleştirmenizi tavsiye ediyoruz çünkü bu hesabınızı korumanın en güçlü yollarından biridir. Artık parolalar hesaplarınızı korumak için yalnız başına yeterli değil, daha güçlü birşeylere ihtiyacımız var. İki adımlı doğrulama (2FA) daha güçlüdür. Parolanızı kullanır, ancak bir aşama daha ekler, ya sizin olan birşey (biometrik) ya da sizin sahip olduğunuz birşey (telefonunuza gelen bir kod ya da akıllı telefonunuza kurulu olan uygulamadan üretilen bir kod).İki adımlı doğrulama sizin için muhtemelen tek ve en önemli koruma adımıdır ve düşündüğünüzden çok daha kolaydır.

3. **Güncelleme**: Bilgisayarınızın, mobil cihazlarınızın, uygulamalarınızın ve Internete bağlı herşeyin üzerinde son versiyon yazılımların kurulu olduğundan ve çalıştığından emin olun. Siber suçlular sürekli olarak kullandığınız teknolojilerin yeni zayıflıklarını bulmaya çalışırlar. Bir zafiyet yakaladıklarında bu zayıf noktaları kullanarak hangi teknolojiyi kullanıyorsanız ona izinsiz girmeye çalışırlar. Eş zamanlı olarak sizin kullandığınız teknolojiyi geliştiren şirketler de yazılımları güncel tutmak için sıkı çalışırlar. Bilgisayarlarınızın ve mobil cihazlarınızın bu güncellemeleri aldığından emin olarak, birilerinin izinsiz bir şekilde sızmasını zorlaştırmış olursunuz. Güncel kalmak için her uygun durumda 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, ya da cihazlarınız eski ise ve artık güvenlik güncellemeleri ile desteklenmiyor ise desteklenen yenisi ile değiştirmenizi öneriyoruz.

4. **Yedekleme**: Bazen ne kadar da dikkatli olursanız olun, cihazlarınız ya da hesaplarınızdan biri ele geçirilebilir. Eğer durum buysa genellikle tek seçenek, bilgisayarınızın ya da mobil cihazınızın kötü amaçlı yazılımlardan arındığından

Güvende Olmak İçin 4 Adım

emin olduktan sonra, tamamen silmek ve baştan yapılandırmaktır. Saldırgan ele geçirdiği sisteminizde, kişisel dosyalarınıza, resimlerinize ve diğer bilgilerinize ulaşımınızı engellemiş bile olabilir. Böyle bir durumda genellikle sizin tek seçeneğiniz yedeklemelerinizi kullanarak tüm kişisel bilgilerinizi geri yüklemek olabilir. Düzenli olarak önemli bilgilerinizin yedeklemelerini yaptığınızdan emin olun ve bu bilgilerin geri yüklenebileceğini doğrulayın. Birçok işletim sistemi ve mobil cihaz otomatik yedeklemeyi desteklemektedir. Ek olarak, siber saldırganlara karşı korumak için yedeklemelerinizi bulut ortamlarında ya da çevrimdışı olarak saklamanızı öneriyoruz.

Daha Fazla Bilgi İçin

Aylık OUCH! güvenlik farkındalığı bültenine üye olun, OUCH! arşivlerine erişin ve securingthehuman.sans.org/ouch/archives 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

Oltalama:	https://securingthehuman.sans.org/ouch/2015#december2015
Parola Yöneticileri:	https://securingthehuman.sans.org/ouch/2015#october2015
İki Adımlı Doğrulama:	https://securingthehuman.sans.org/ouch/2015#september2015
Parolalar:	https://securingthehuman.sans.org/ouch/2015#april2015
Yedeklemeler:	https://securingthehuman.sans.org/ouch/2015#august2015

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