Herkes İçin Aylık Güvenlik Farkındalığı Bülteni

Güvenli Olmanın Dört Basit Adımı

Genel Bakış

Teknolojiden en güvenli şekilde faydalanmak çok zor ve kafa karıştırıcı görünebilir. Ancak hangi teknolojiyi kullandığınıza veya onu nasıl kullandığınıza bakılmaksızın, güvenli kalmanıza yardımcı olacak dört basit adım aşağıda listelenmiştir:

1. Siz: Birincisi ve en önemlisi, tek başına teknoloji sizi tam olarak koruyamaz, en iyi savunma kendinizsiniz. Saldırganlar, istediklerini elde etmenin en kolay yolunun bilgisayarınız veya diğer cihazlar yerine sizi hedef almak olduğunu öğrendiler. Parolanızı, kredi kartınızı veya bilgisayarınızın kontrolünü ele geçirmek istiyorlarsa, genellikle bir aciliyet duygusu oluşturarak, vermeniz için sizi kandırmaya çalışırlar. Örneğin, gerçekte yalnızca bilgisayarınıza erişmek isteyen siber-suçlular oldukları halde sizi Microsoft teknik destek ekibi gibi davranarak arayabilir ve bilgisayarınıza virüs bulaştığını iddia edebilirler. Belki de size paketinizin teslim edilemediğine dair bir e-posta gönderir ve posta adresinizi doğrulamak için bir bağlantıyı tıklatmanız konusunda size baskı yaparlar, gerçekte bilgisayarınızı ele geçirmek için kötü amaçlı bir web sitesini ziyaret etmenizi sağlarlar. Sonuçta, saldırganlara karşı en büyük savunma silahınız yine kendinizsiniz. Sağduyu kullanarak birçok saldırıyı tespit edebilir ve durdurabilirsiniz.

2. Parolalar: Günümüz işlemci hızları, eski, 8 karakterli şifreyi modası geçmiş ve savunmasız bıraktı. Bir site sizden parola oluşturmanızı istediğinde, bunun yerine güçlü ve benzersiz bir parola oluşturun. Bir parola, "YağmurYağıyorSellerAkıyor" gibi hatırlanması kolay bir dizi kelimeyi kullanan bir parola türüdür. Parolanız ne kadar uzunsa, o kadar güçlüdür. Benzersiz bir parola, her cihaz veya çevrimiçi hesap için farklı bir parola kullanmak anlamına gelir. Bu şekilde bir parolanız tehlikeye girerse, diğer tüm hesaplarınız ve cihazlarınız hala güvendedir. Bütün bu parolaları hatırlayamıyor musunuz? Tüm parolalarınızı şifreli bir biçimde (ve daha birçok harika özellik de dahil) güvenli bir şekilde saklayan bir parola yöneticisi uygulaması kullanın.

Son olarak, iki adımlı doğrulamayı etkinleştirin (ayrıca iki faktörlü veya çok faktörlü kimlik doğrulama olarak da bilinir). İki adımlı doğrulama parolanızı kullanır, bunun yanında akıllı telefonunuza gönderilen bir kod veya sizin için kodu oluşturan bir uygulama gibi ikinci bir adım daha ekler. İki adımlı doğrulama, muhtemelen çevrimiçi hesaplarınızı korumak için atabileceğiniz en önemli adımdır ve kullanımı düşündüğünüzden çok daha kolaydır.

3. Güncelleme: Bilgisayarlarınızın, mobil cihazlarınızın, programlarınızın ve uygulamalarınızın her birinin yazılımının en son sürümünü kullandığından emin olun. Siber saldırganlar, cihazlarınızın kullandığı yazılımlarda sürekli olarak yeni güvenlik açıkları ararlar. Güvenlik açıklarını keşfettiklerinde, istismar etmek ve kullandığınız cihazları ele geçirmek için özel programlar kullanırlar. Tüm bunlar olurken, bu aygıtlar için yazılımı yapan şirketlerin durumu fark edip güncellemeler yayınlayarak zafiyetleri düzeltmesi çok zordur. Bilgisayarlarınızın ve mobil cihazlarınızın bu güncelleştirmeleri derhal yüklemesini sağlayarak bir siber saldırganın cihazlarınızı ele geçirmesini zorlaştırabilirsiniz. Güncel kalmak için, mümkün olduğunda otomatik güncellemeyi etkinleştirmeniz yeterlidir. Bu kural, İnternet bağlantılı TV'ler, bebek monitörleri, güvenlik kameraları, evinizde kullandığınız ağ yönlendiricileri, oyun konsolları ve hatta arabanız da dahil olmak üzere bir ağa bağlı neredeyse tüm teknolojiler için geçerlidir.

4. Yedeklemeler ve Geri Dönüş: Bazen, ne kadar dikkatli olursanız olun, cihazlarınız kötü niyetli kişiler tarafından ele geçirilmiş olabilir. Bu durumda, kişisel bilgilerinizin tümünü geri yüklemenin tek yolu yedeklerinizdir. Önemli bilgileri düzenli olarak yedeklediğinizden emin olun ve verilerinizi yedeklerinizden geri yükleyebileceğinizi doğrulayın. Çoğu işletim sistemi ve mobil cihaz, harici sürücülere veya buluta otomatik yedeklemeleri desteklemektedir.

Türkçe Çevirisi

Selma Süloğlu, ODTÜ Bilgisayar Mühendisliğinde doktorasını tamamlamış olup Hawaii Üniversitesinde yazılım mimarileri ve yazılım güvenliği üzerinde doktora sonrası araştırma yapmaktadır.

Sema Yüce, Türkiye'nin önde gelen kurumsal şirketlerinde ve özellikle bilişim, finans, telekomünikasyon, sigortacılık, sanayi, perakendecilik gibi sektörlerde; bilgi güvenliği, uyum, BT yönetişim/strateji, risk yönetimi, iş sürekliliği, hizmet yönetimi, altyapı hizmetleri, yazılım geliştirme ve program/proje yönetimi alanlarında yönetici ve danışman olarak 19 yılı aşkın süre görev yaptıktan sonra, Truth ISC (www.truth-isc.uk) adıyla kurduğu Türkiye ve İngiltere'de faaliyet gösteren danışmanlık şirketinde hizmet vermeye devam etmektedir.

Konuk Editor

*SANS'ın sertifikalı eğitmeni olan **Steve Anson**, dünya çapında IT güvenlik ekiplerine ve resmi kurumlara güvenli duruşlarını geliştirmek için danışmanlık yapmaktadır. Steve yakında yayınlanacak olan Applied Incident Response kitabının yazarıdır ve BT güvenlik uzmanlarına www.AppliedIncidentResponse.com adresinden ücretsiz kaynaklar sunmaktadır.*

Kaynaklar

Sosyal Mühendislik:	https://www.sans.org/u/W3G
Kişiye Özel Dolandırıcılık:	https://www.sans.org/u/W3Q
Parolaları Basitleştirmek:	https://www.sans.org/u/W3V
Yedeklemiş miydiniz? :	https://www.sans.org/u/W40