Bilgisayar Kullanıcıları için Aylık Güvenlik Farkındalığı Bülteni

OUCH!

BU SAYIDA...

- Genel Bakış
- Parolalar
- İki-Adımlı Doğrulama (Two-Step Verification)

İki-Adımlı Doğrulama

Genel Bakış

Bilgiyi korumanın anahtarı, kim olduğunuzu kanıtlama yani kimlik doğrulama (authentication) sürecidir. Güçlü kimlik doğrulama, e-postalarınız, fotoğraflarınız ya da banka hesaplarınız gibi size ait olan bilgilere sadece sizin erişmenizi garanti etmeye çalışır. Kim olduğunuzu doğrulamanın 3 değişik yolu vardır : "bildiğiniz bir şey : örneğin bir parola", "sahip olduğunuz bir şey : örneğin sürücü belgesi numaranız", "sizin olan bir şey : örneğin parmak iziniz". Bu yöntemlerin her birinin avantaj ve dezavantajları vardır. En yaygın yöntem "bildiğiniz bir şey" olan "parolalar"dır. Bu bültende sizlere kendinizi, "sadece parola" kullanmaktan çok daha güvenli ve kullanımı çok basit bir yöntem olan, "iki-adımlı doğrulama" ile nasıl koruyacağınızı anlatacağız. İki-adımlı doğrulamayı daha iyi anlamak için, önce parolalardan başlamalıyız.

Konuk Yazar

Keith Palmgren Bilgi Güvenliği alanında 30 yılı aşkın tecrübeye sahiptir. SANS Enstitüsü Sertifikalı Eğitmeni ve 5 günlük "SANS SEC301 Bilgi Güvenliğine Giriş" kursunun yazarıdır. Eğitmenliğin dışında Keith danışmanlık yapmakta ve projeler yazmaktadır. Keith'i **@kpalmgren** hesabından takip edebilirsiniz.

Parolalar

Parolalar, kim olduğunuzu "bildiğiniz bir şey" üzerine dayanarak kanıtlar. Parolaların tehlikeli yanı, onların birer "tekil problem noktası (single point of failure)" oluşturmasıdır. Eğer birisi parolanızı tahmin ederse ya da erişebilirse, sizin yerinizi alabilir ve o parola ile korunan tüm bilgiye erişebilir. İşte bu nedenle size, parolalarınızı başkalarının tahmin etmesi zor olan güçlü parolalar seçerek, her bir hesap için farklı parolalar kullanarak ve asla hiç kimseyle parolalarınızı paylaşmayarak korumanız gerektiği öğretilir. Bu tavsiyeler hala geçerliliğini korumasına rağmen parolalar bugünün modern çağında etkinliklerini ve kullanışlılıklarını kaybediyor. Son teknolojiler siber saldırganların parolaları ele geçirmelerini çok kolaylaştırdı. Güçlü kimlik doğrulama için ihtiyacımız olan kullanımı kolayve daha güvenli bir çözüm. Neyse ki, iki adımlı doğrulama olarak adlandırılan ve yaygın olarak kullanılan bir alternatif var.

İki-Adımlı Doğrulama

İki-adımlı doğrulama (bazen iki-faktörlü doğrulama (2FA) olarak da adlandırılır) sadece parola kullanmaktan çok daha güvenli bir çözümdür. Bu çözüm sadece bir değil, iki değişik doğrulama yöntemi kullanır. Bir örnek sizin banka kartı kullanımınız olabilir. Bir ATM'den para çekmek istediğinizde, iki-adımlı doğrulama yöntemi kullanırsınız. İhtiyacınız olan iki şey vardır : Banka

İki-Adımlı Doğrulama

kartınız (sahip olduğunuz birşey) ve PIN kodunuz (bildiğiniz birşey). Eğer banka kartınızı kaybederseniz, paralarınız hala güvendedir. Kartınızı bulan her kimse, PIN kodunuzu bilmediği sürece paranızı çekemez (tabii eğer PIN kodunuzu kartın üzerine yazmadıysanız, ki bu çok kötü bir fikirdir). Aynı şey, PIN kodunuzu bulan birisi kartınıza sahip olmadığında da geçerlidir. Saldırganın her ikisine de ihtiyacı vardır. İki-adımlı doğrulamayı çok daha güvenli yapan budur, size iki katmanlı güvenlik sunar.

İki-adımlı doğrulamayı mümkün olan her zaman kullanın, bilgilerinizi korumak için atabileceğiniz en güçlü adımlardan biridir.

İki Adımlı Doğrulama Kullanımı

İki-adımlı doğrulama her bir hesabınız için ayrı ayrı yapmanız gereken bir şeydir. Neyse ki, birçok çevrimiçi hizmet şu an bu yöntemi destekliyor. Bu alandaki liderlerden birisi de Google. Google hesapları siber saldırganların öncelikli hedefi, çünkü birçok ücretsiz ve çevrimiçi hizmeti dünyanın her yerinden milyonlarca insan sunuyor. Bu nedenle Google güçlü bir doğrulama sunmak durumundaydı ve çevrimiçi hizmetleri için iki-adımlı doğrulama kullanan ilk organizasyonlardan biri oldu. Eğer Google'ın iki-adımlı doğrulamasının nasıl çalıştığını anlarsanız, Twitter, Facebook, Apple, Instagram gibi birçok diğer sitenin ve bankaların da nasıl çalıştığını anlayacaksınız.

İlk önce, Google hesabınızı açın ve iki-adımlı doğrulamayı aktif hale getirin ve mobil telefon numaranızı kaydedin. Bunu yaptığınızda, iki-adımlı doğrulama şu şekilde çalışacaktır. Tıpkı eskiden olduğu gibi hesabınıza kullanıcı adı ve parolanızla bağlanacaksınız. Bu iki-adımlı doğrulamanın ilk faktörüdür – bildiğiniz bir şey. Sonra Google kaydettiğiniz telefon numaranıza 6 karakterli tekil bir kod içeren bir SMS metin mesajı iletecek. Parolanız gibi, bu 6 karakteri de gireceksiniz. Bu da iki faktörün ikincisidir. Böylece, hesabınıza başarı ile bağlanmak için hem parolanıza, hem de tekil kodları alabilmeniz için gereken cep telefonunuza sahip olmalısınız. Bir saldırgan, parolanıza sahip olsa bile, telefonunuza da sahip olmadığı sürece, Google hesabınıza giremeyecektir. Hesabınızın gerçekten güvende olduğundan emin olmak için Google, her bağlanmaya çalıştığınızda yeni ve tekil bir kod gönderecektir.

Google ve birçok diğer sitede, iki-adımlı doğrulama için başka bir seçenek daha var. Tekil kodları SMS metin mesajları ile almak yerine, akıllı telefonunuza bir doğrulama uygulaması kurabilirsiniz. Bu uygulama her bağlanmak istediğinizde tekil kod üretecektir. Bu yöntemin avantajı, bir telefon hizmet sağlayıcısına ihtiyaç duymadan telefonunuzun bu tekil kodları üretebilmesidir. Ek olarak tekil kod, yerel olarak telefonunuz üzerinde üretildiği ve size gönderilmediği için, araya girilerek ele geçirilemez.

Lütfen hatırlayın, iki-adımlı doğrulama kendiliğinden aktif değildir, onu siz aktif hale getirmelisiniz. Başlangıçta size daha zor gibi görünse de, mümkün olan her zaman özellikle de e-postalarınız, çevrimiçi bankacılık ya da bulut üzerinden kullandığınız

İki-Adımlı Doğrulama

dosyalama hizmetleri gibi kritik hizmetler için kullanmanızı kesinlikle öneriyoruz. İki-adımlı doğrulama bilgilerinizi sadece parolalarla korumaktan çok daha güvenlidir.

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.

Mustafa Emrah Ünsür, Güvenlik Araştırmacısı olarak araştırmaları, makaleleri ve çevirileri vardır. Beyaz Şapkalı Hacker olarak kendisi tarafından kodlanan ve kodlanmakta olan 'exploit'ler ve 'tool'lar bulunmaktadır. Ayrıca, Sızma Testi Uzmanı olarak özel şirketlere ve devlet kurumlarına Zafiyet ve Sızma Testi yapmış ve yapmaya devam etmektedir.

Kaynaklar

Parolalar:	http://www.securingthehuman.org/ouch/2015#april2015
İki-Adımlı Doğrulamayı Destekleyen Siteler:	https://twofactorauth.org
Stop|Think|Connect:	http://stopthinkconnect.org/2stepsahead
Google İki-Adımlı Doğrulama:	http://www.google.com/landing/2step/
SANS Günün Bilgi Güvenliği İpucu:	http://www.sans.org/tip_of_the_day.php