GÜVENLİ GÜNLER BÜLTENİ

Bilgisayar kullanıcılarına yönelik hazırlanır. Her ayın 15'i çıkar. Diğer sayılara erişmek ve sonraki mesajların direk posta kutunuza gelmesi için guvenligunler.com adresini ziyaret ediniz.

HAZİRAN 2017

Sosyal Mühendislik Saldırıları Nasıl korunuruz?

Bugüne kadar eminim herkes, en az bir kez, kurumsal veya kişisel e-posta adresleri üzerinden sosyal mühendislik saldırısına hedef olmuştur. Şanslı ve biraz bilgili olanlarımız saldırılardan zarar görmeden kurtulmuştur, ancak bu saldırıların tuzağına düşmüş olan kişi sayısı da bir o kadar fazladır.

Günümüzde sistemler tarafından alınan önlemler dışarıdan gelecek zararı büyük ölçüde engellemektedir ama özellikle kurumlar boyutunda ne yazık ki en zayıf halka olan insan hedef haline gelmiştir. Sistemsel olarak ne kadar önlem alınmış olursa olsun, hedef haline gelen insanın bir anlık dalgınlığı veya bilinçsiz davranışından dolayı güvenliği sağlamak tam anlamıyla mümkün olamamaktadır.

SOSYAL MÜHENDİSLİK NEDİR?

Sözlük anlamıyla sosyal mühendislik, internette insanların zayıf yanlarından yararlanarak çeşitli ikna ve kandırma yöntemleriyle istenilen bilgileri elde etmeye çalışmaktır. İnsanların karar verme süreçlerini değiştirmeye yönelik teknikler içerir.

Bu sözlük karşılığı son derece doğrudur ama eksiktir; birkaç nokta atlanmıştır. Saldırganlar, insanların korku, heyecan, endişe veya panik gibi, düşünmelerini engelleyen, kararlarını etkileyen duyguları kullanarak hedeflerini kandırmaya çalışırlar. Sosyal mühendislik saldırıları, kimi zaman bir borç, kimi zaman aksayan bir iş, kimi zaman ise tanıdık birinden gelen yardım isteği olarak karşımıza çıkmaktadır. En sık rastlanılan örnekler teslim edilemeyen kargo e-postaları ve ödenmeyen fatura e-postalarıdır.

Sosyal mühendislik saldırılarının en hedefe yönelik ve akıllıca yapılandırılmışları ise, önceden hazırlanmış, hedef kişinin sosyal medya hesapları veya çalıştığı kurum ile ilgili bilgiler üzerinden ön çalışmalara göre hazırlanmış olan saldırı senaryolarıdır. Bu saldırılar toplu hedeften çok tek bir kişiye yönelik yapılmış olduklarından, kişilerin saldırganların tuzağına düşme olasılığı çok yüksektir.

Saldırı yapmanın, bilgilere göre içerik hazırlamanın ve gerçekleştirmenin bu kadar kolay olduğu bir dünyada biz kullanıcılar olarak nelere dikkat etmeliyiz, ne gibi önlemler almalıyız?

Sosyal Mühendislik Saldırılarından Korunmak İçin İpuçları

» Sosyal medya hesaplarınız üzerinden paylaştığınız içeriklere ve kimlerin sizlere ait bilgilere erişebildiğine dikkat edin, profillerinizi kısıtlı kullanın ve tanımadığınız kişilerden gelen arkadaşlık isteklerini kabul etmeyin,
» Gönderen kişiyi tanıyor musunuz; gönderen kişinin görünen adına inanmayın, gönderici adresini kontrol edin, tanımıyorsanız dikkate almadan silin,
» E-postanın yazım dilini kontrol edin; imla hataları veya anlam düşüklüğü varsa büyük olasılıkla sahte bir e-postadır,
» E-posta genele hitaben mi gönderilmiş yoksa kişisel olarak adınıza mı gönderilmiş kontrol edin; saldırı e-postaları genellikle kişiye hitaben değil genele hitaben oluşturulur,
» E-postalarla istenen bilgileri iletmeden önce şüpheniz varsa teyit edin,
» Özellikle bankacılık işlemleri ile ilgili gönderilen e-postalar içinde yer alan bağlantıları ve dosyaları kesinlikle tıklamayın, uygulamaları kurmayın,
» E-posta içinde yer alan adres *link*'leri gerçekten belirtilen adrese mi gidiyor, üzerine tıklamadan kontrol edin, mümkünse bağlantıyı tıklamak yerine *browser* üzerinden kendiniz adresi yazarak erişim sağlayın,
» E-posta içindeki açılan sitelere veya *pop-up* pencerelere kesinlikle bilgilerinizi girmeyin,
» E-posta ekinde gelen dosyayı açmak istediğinizde çalıştırmak için izin isteyen uygulamaları asla bilgisayarınıza kurmayın,
» Unutmayın, bankalar ve kurumlar kişisel bilgilerinizi asla e-posta yoluyla istemezler,
» Gönderen kişinin imza, kurum ve iletişim bilgilerini kontrol edin,
» E-postada her şey yolunda gibi görünüyor olsa bile görünüşe aldanmayın; en ufak şüphede bile söz konusu e-postayı dikkate almayın, açmayın, tıklamayın ve silin.

REFERANS

Wikipedia (https://tr.wikipedia.org/wiki/Sosyal_m%C3%BChendislik)

YAZAR HAKKINDA

Nilay Ersen Bozacıoğlu 1983 yılında İstanbul'da doğdu. Yeditepe Üniversitesi Sistem Mühendisliği bölümü'nden mezun oldu. Bankacılık ve Telekom sektöründe Bilgi güvenliği alanında özellikle Bilgi Güvenliği Farkındalık çalışmaları ile ilgili 9 yıldır görev yapmaktadır.