Sosyal Mühendislik,

Bir bilgisayar sisteminin kullanıcılarını, bir bilgisayar sistemine yetkisi olmadan erişim elde etmek için gizli bilgileri açığa çıkarma sanatıdır. Bilgisayar korsanları yani Hackerlar kimliğini kullanan kullanıcıları hayati oturum açma bilgilerini serbest bırakmaları için kullandığı hileleri bilmek, bilgisayar sistemlerini korumak açısından temel bir gerekliliktir.

SOSYAL MÜHENDİSLİK RİSKLERİ

- Sosyal mühendislik saldırıları temelde insan ve bilgisayar hedefli olmak üzere iki ana başlığa ayrılıyor.
- İnsan hedefli saldırılarda saldırgan kurbanla yüz yüze gelir. Fakat burada el ve kol hareketlerinden jest ve mimiklerinden kaynaklı kendilerini ele vermeleri olağan olduğundan yüz yüze gelmeyi pek tercih etmezler.
- Kurbana bir bilgisayar, mobil cihazı gibi vektörler tercih edilir. Bu saldırı şekli görece daha etkilidir ve az risk taşır bununla birlikte saldırganın yakalanma ihtimalini daha da azaltır. Bu nedenle sosyal mühendislik saldırılarında tercih edilen yöntem bilgi teknolojilerinin kullanılması olmaktadır.

Sosyal Mühendisler;
Sizin değersiz görüp çöpe attığınız kağıtlardan, fişlerden bütün kimlik bilgilerinize ve gittiğini yerlere kadar her yere ulaşmaktadırlar.

SOSYAL MÜHENDİSLER HANGİ YOLLARI İZLER

- Mağdur edecekleri kurbanları hakkında bilgi toplarlar ve plan yaparlar.
- Hatta A planının ötesinde B planı, C planı gibi olası bir hata durumunu kurtarabilmek için yedek planlar bulundururlar.
- Toplanan bilgi, saldırı zamanı geldiğinde aşamalı olarak uygulanır.
- İnsanların zayıf yönlerini bulurlar, yumuşak karınlarına dokunurlar.
- Şahsi ve özel bilgilerini öğrenirler, kişi hakkında bilgi toplarlar. Bunlara örnek olarak ad, soyad, adres bilgileri, ilgi alanları, korktukları hayvanlar, yakın arkadaşları gibi birçok unsur sıralanabilir.
- Dikkatli davranmamız gereken konulardan biri **bu stratejilere hemen kanmayıp, inceleme yapmadan bilgilerimizi paylaşmamaktır.**

Olası Mağdurların Psikolojik Tepkileri

- Bilgisayarımızda önemli bir verinin olmadığını savunarak önlem almayabilir ve farkında olmadan saldırganın hedefine ulaşmasını sağlayabiliriz. Bu duruma ünlü Titanik gemisinin asla batmayacağı inancına sahip olan yöneticilerin önlem almaması durumunda buzdağına çarpması olayından yola çıkılarak "Titanik Sendromu" adı verilmektedir.
- Sosyal mühendislik mağdurlarında oluşan bir diğer tepki ise inkar savunma mekanizmasıdır. Bu mekanizmaya sahip olan birey bilgisayarında güvenlik yazılımı olduğu için kendini aşırı güvende hissedebilir ve böylece kaygı seviyesinin çok düşük olması sonucu saldırganın hedefine ulaşmasında etkin rol oynamaktadır.

Sosyal mühendislik saldırılarından nasıl korunabilirsiniz?

- Her gönderilen linke tıklamayın
- Dikkatli olun, dikkatle inceleyin.
- Özel bilgilerinizi verirken seçici davranın.
- Zorunda değilseniz, bilgilerinizi paylaşmayın. Karşıdaki kişinin bilgilerinizi aleyhinize kullanıp kullanmayacağını bilemezsiniz.
- Yapılabilecek en küçük hata bile size çok büyük felaketlere dönüş yapabilir.
- Farkındalığınızı arttırmalı ve çevrenizdeki insanları da bu konuda bilgilendirmelisiniz.
- Eğer yöneticiyseniz bir kurumda, çalışanlarınızı sosyal mühendislik ve bilgi güvenliği konusunda eğitim vermeniz gerekmektedir.