SOSYAL MÜHENDİSLİK

Siber güvenliği ciddi anlamda tehdit eden ve güvenlik önlemlerinin aşılmasını kolaylaştıran en önemli unsurların başında insan faktörü gelmektedir. Sosyal mühendislikte de teknik altyapılar ve sistemler yerine insanların zafiyetleri kötüye kullanılmaktadır.

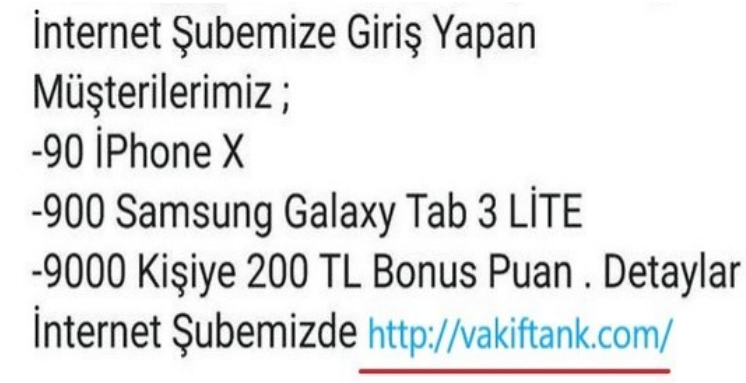
"Zincir en zayıf halkası kadar güçlüdür. Burada ise en zayıf halka insandır."

Sosyal Mühendislik Nedir?

Sosyal mühendislik, saldırganın istediği şekilde davranmanızı sağlayan psikolojik bir saldırı türüdür. İnsanların tanımadıkları biri için yapmayacakları şeyleri yapmalarını sağlama sanatıdır. Teknoloji kullanımından çok insanların hile ile kandırılarak bilgi elde edilmesidir.

İnsanlar kandırılma ihtimalinin çok düşük olduğunu düşünür. Bu ortak inancın farkında olan saldırganlar, isteklerini çok akıllıca sunarak hiç kuşku uyandırmadan kurbanların güvenini sömürürler.

Aldatmak, kandırmak, dolandırmak gibi kavramlar binlerce yıldır var olmuş kavramlardır. Ancak saldırganlar bu tekniği dijital ortamda kullanmanın da son derece etkili olduğunu keşfetmiştir. Bu tekniğin nasıl kullanıldığını anlamak için günümüzde yaygın olan örneklerine bakmakta yarar vardır.



⇒ Kendilerini "polis", "asker", "savcı" olarak tanıtanlar"

⇒ Ödül Kazandınız" gibi mesajlar göndererek insanlardan bilgi ya da para talep edenler

Sosyal Mühendislik; basit tarifiyle dolandırıcılığa benzese de, genelde bilgi sızdırmak veya bir bilişim sistemine sızmak için kullanılabilen bir yöntemdir. Bu yöntemde genel olarak saldırgan mağdur ile yüz yüze gelmez. Kötüye kullanılan unsur ise sistem zafiyetleri değil insan zafiyetleridir.

Zafiyetlerden yola çıkarak örneklendirmek gerekirse, kurumların ya da kişilerin çöplerinde bulunabilecek imha edilmemiş dokümanlar üzerinde bulunan ve geçerliliğini yitirmemiş bilgiler sayesinde kurumlar ve kişiler hakkında önemli bilgilere ulaşılabileceğinden bahsedilebilir.

- Bilginiz başkalarının eline geçebilir.
- Bağlı olduğunuz kurum veya kuruluşun onuru, toplumdaki imajı zarar görebilir.
- Donanım, yazılım, veri ve kurum çalışanları zarar görebilir.
- Önemli verilere erişim engellenebilir, parasal kayıplar ve vakit kaybı yaşanabilir.

Sosyal Mühendislik Teknikleri

- Omuz Sörfü
- Çöp Karıştırma
- Truva Atları
- Rol Yapma
- Oltalama
- Tersine Sosyal Mühendislik

Sosyal Mühendislik Sızma Hedefleri

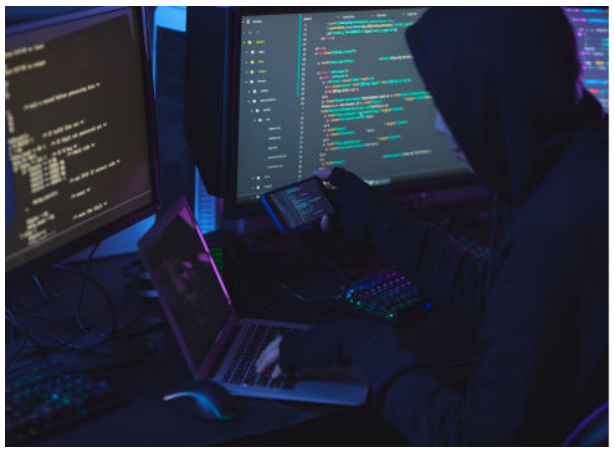
- Sistemi Ele Geçirme
- Kritik Bilgilere Erişim
- Hedef Sistemlere Erişim Sağlama
- Yönetici Hakkı Elde Etme
- Sistemde Kalıcı Olma
- Gizlilik

Sosyal Mühendislik Sızma Çeşitleri

- Fiziksel Sosyal Mühendislik
- Telefon İle Sosyal Mühendislik
- Mail Yoluyla Sosyal Mühendislik

Kendimizi Nasıl Koruruz?

Kendinizi korumak için ilk olarak yapmanız gereken, sosyal mühendislik saldırılarının nasıl tespit edileceğini, engelleneceğini, durdurulacağını öğrenmektir.



Biri veya birilerinin sizi hedef almaya çalıştığından şüpheleniyorsanız, o kişi ile bir daha asla iletişim kurmayın. Sizinle telefon hattı üzerinden irtibat kuruyor ise telefonu kapatın. Eğer çevrimiçi sohbette iseniz bağlantınızı sonlandırın. Eğer güvenmediğiniz bir yerden gelen bir e-posta ise, eklentilerini indirmeyin ve bahse konu e-postayı silin. Eğer çalıştığınız kurum veya iş yeri ile ilgili bir saldırı olduğunu düşünüyorsanız, işyerindeki yardım masasına ya da ilgili güvenlik uzmanlarına haber verin. Bütün bu aşamalarda kaydedeceğiniz ekran görüntüleri sonraki süreçte oldukça önem arz edecektir.

Olası Saldırıları Engellemek İçin Ne Gibi Önlemler Alınmalı?

Kişisel/Özel Bilgilerinizi Paylaşmayın: Saldırganlar hakkınızda ne kadar çok bilgiye sahip olursa size o kadar kolay ulaşıp istediklerini yaptırmak için sizi yanlış yönlendirebilir. Her bilgi internet ortamında paylaşılmamalıdır. Kendinizle ilgili basit gördüğünüz paylaşımlarınız, hayatınızın bütünü hakkında bilgi sahibi olmak amacıyla kötü niyetli kişilerce zamanla bir araya getirilebilir. Ne kadar az bilgi paylaşırsanız (forum siteleri, e-posta adresleri ya da sosyal medya siteleri) saldırıya uğrama riskiniz de o kadar az olur.

Şifrelerinizi Paylaşmayın: Hiçbir kurum ya da kuruluş şifrenizi sormak için sizinle iletişime geçmez. Eğer birileri size şifrenizi soruyorsa bu bir sosyal mühendislik saldırısıdır.

Sizinle İrtibat Kuran Kişileri Sorgulayın: Bankanızdan ya da servis sağlayıcınız gibi kuruluşlardan aranabilirsiniz. Arayan kişi hakkında herhangi bir şüpheniz varsa arayan kişinin adını ve ona ulaşabileceğiniz bir numarayı isteyerek güvenilir bir kaynaktan kuruluşa ait telefon numarasını bulabilirsiniz. (Örneğin banka hesap özetinizde yazan numaradan ya da telefon faturanızda bulunan numaralardan) Böylece bahse konu kurumu ya da şirketi aradığınızda gerçekten yetkili personel ile konuştuğunuzdan emin olabilirsiniz.

URL/Adres Kontrolü Yapın: Oltalama saldırılarında oltaya takılmamanın en önemli unsurlarından biriside tarayıcıda bulunan adresi kontrol etmektir. Adres çubuğunda göz kaçırılan bir karakter değişikliği istenmeyen sonuçlara yol açabilir.

Güvenilir Olmayan Kaynaklara Dikkat Edin: Bir dosya indirmek istediğinizde güvenilir kaynaklardan ve mümkünse doğrulanmış yapımcılardan indirmelisiniz ve bilgisayarınızda düzenli olarak virüs taraması yapmalısınız.

Kurum İçinde Periyodik Olarak Bilgi Güvenliği Testleri Yapın: Kurum çalışanları periyodik olarak bilgi güvenliği eğitimleri almalı ve sızma testlerine tabi tutulmalıdır. Tüm bilgisayarlara antivirüs yazılımları kurulmalı, çöpe atılması gereken dokümanlar, mutlaka kırpma makinelerinden geçirilmelidir. Kuruma ziyaretçi olarak gelen kişilerden kimlik alınarak kurum çalışanları tarafından refakat edilmelidir.

"En güvenli bilgisayar internet bağlantısı olmayan ve kapalı olandır. Ancak bir ihtimal var ki; saldırganlar ofise gidip bilgisayarı açması için birini ikna edebilir."