



SOSYAL MÜHENDİSLİK SALDIRILARI

Can Bican
Uzman Araştırmacı
bican@uekae.tubitak.gov.tr
0312 468 53 00

- Sosyal mühendislik nedir?
 - Yöntemleri?
 - Oluşturabildiği tehditler?
 - Alınabilecek önlemler?

- İnsan faktörü içermeyen bir bilgisayar sistemi yoktur.
- **Kevin Mitnick:** Pentagon, Sun Microsystems, Motorola gibi birçok yeri kırarak FBI'ın en çok arananlar listesine giren ilk hacker.

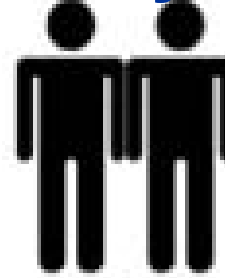
“Güvenlik zincirindeki en zayıf halka insandır.”

Bilgisayar güvenliği terimleriyle **Sosyal Mühendislik**, insanlar arasındaki iletişimdeki ve insan davranışındaki modelleri *açıklıklar* olarak tanıyıp, bunlardan faydalanarak güvenlik süreçlerini atlatma yöntemine dayanan müdahalelere verilen isimdir.

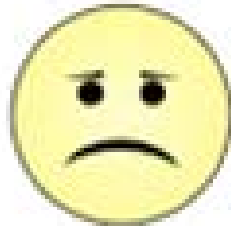
1. Bilgi Toplama



2. İlişki Oluşturma



4. Uygulama



3. İstismar



- Sahte senaryolar uydurmak (pretexting)
- Güvenilir bir kaynak olduğuna ikna etmek (phishing)
- Truva atları (trojan)
- Güvenilir bilgi karşılığında yardım, para, eşantiyon, hediye, ... önermek
- Güven kazanarak bilgi edinmek
- Omuz sörfü, çöp karıştırmak, eski donanımları kurcalamak

From: Komiser Kolombo

To: Ben

Bu email adresinden yüksek düzey bir bürokrata küfür içerikli mesaj atılmıştır. Konuyu incelemem için mesajı alır almaz şifrenizi yollamanız gereklidir.

- Genellikle e-posta üzerinden gerçekleşen bir yöntemdir.
- Saldırgan, amacına ulaşmak için güvenilir ya da doğruluğu sorgulanamaz bir kaynaktan geldiğine inandırır.
- Hedef, saldırılanı bilgi vermeye zorlamak ya da hatalı bir hareket yapmaya (sahte web sitesine tıklamak, virüslü yazılım kurmak, ...) yönlendirmektir.

Tebrikler! Çekilişimizi kazandınız. Parayı yollamamız için lütfen bize hesap numaranızı ve doğum tarihinizi gönderin.

- Hassas bilgiye ulaşmak için, kişinin hassasiyetlerini kullanan bir yöntemdir.
 - Kurban, sonunda karlı (ya da zarar görmeden) çıkacağına ikna edildiği bir senaryoyla hassas bilgiyi verebilir, ya da saldırgan yerine zararlı işlemler yapabilir.
 - Hediyeli anket,
 - Ödüllü soru,
 - ...

Yıllar sonra Facebook'tan ilkokul arkadaşım ile karşılaştım. O da sistem yöneticisiymiş. Sabaha kadar Msn'den mesleğimiz hakkında konuştuk.

- Saldırganın hedefine, iş dışında ya da iş sırasında güvenini sağlayacak şekilde iletişime geçip ikna ederek bilgi vermesine ya da istediğini yaptırmasına dayanan bir yöntemdir.
 - Şirket/kuruma sağlayıcı olarak yaklaşım erişim hakkı olan personelle güvene dayanan arkadaşlık kurmak
 - İş dışında oluşan ilişkileri suistimal etmek
 - Kurbanla ortak ilgileri / beğenileri paylaşıyor izlenimi vererek güven sağlamak

- Omuz sörfü -- Şifreyi yazarken, erişimi kısıtlı sistemlere erişirken kurbanı izlemek
- Çöp karıştırmak -- Çöpe atılmış CD, disket, kağıt, ajanda, not, post-it, ... gibi eşyaları incelemek
- Eski donanımları kurcalamak -- Hurdaya çıkmış, ikinci el satış sitelerinde satışa sunulmuş, çöpe atılmış, kullanılmadığı için hibe edilmiş donanımın içeriğini incelemek

- Yetkisiz Erişim
- Hizmet Hırsızlığı
- İtibar ve Güven Kaybı
- Dağıtık Hizmet Engelleme
- Hassas Bilgiye Erişim
- Veri Kaybı
- Yasal Yükümlülükler
- Hukuki Yaptırım ya da Cezalar

- Artırılmış Fiziksel Güvenlik
- Etkili Güvenlik Politikaları
- Güvenliğe Aykırı Davranışların Uyarılması
- Detaylı Olay Müdahale Yöntemleri
- Denetleme

- Fiziksel güvenlik ve yerel / konsoldan erişim güvenliği genellikle uzaktan erişime göre olma olasılığı daha az görülür.
 - Sisteminize fiziksel erişimi olan herkese güveniyor musunuz?
 - Bütün kullanıcılarınıza güveniyor musunuz?
 - ...
 - Elektrikler kesildiğinde kart erişiminiz nasıl çalışıyor?

- Güvenlik politikaları açık, anlaşılır, mantığa uygun, uygulanabilir, erişilebilir ve kapsayıcı olmalıdır.
- Kurumla çalışanları ve sağlayıcıları arasındaki güvenlik ilişkisi belirlenmelidir.
- Azı mı, çoğu mu zarar?



- Çalışanlar politikalar hakkında ne kadar bilgiliyse, güvenlik politikaları o kadar değerlidir.
- Üst yönetim, tüm çalışanların güvenlik kontrollerine uymaları için gerekeni yapmaya kararlı olmalıdır.
- Eğitimle birlikte gelen yaptırımlar, çalışanların güvenlik politikalarını izlemesini sağlar.

- Bir sosyal mühendislik saldırısı sırasında yapılacakların belirlenmesi özellikle önemlidir.
 - E-posta mesajlarının asıl kaynağı,
 - Web adreslerinin kimlik doğrulama yöntemleri,
 - Telefonlarda arayan bilgisinin belirlenmesi,
 - Olay meydana geldikten sonra durumun yetkili personele iletilmesi.

- Bilgi Toplama
 - Kurumsal web sayfaları
 - Arama motorları
 - Haber grupları / forumlar
 - İş arama siteleri
 - Sosyal ağ siteleri (orkut, facebook, linkedin, ...)
 - Sarı sayfalar

- Fiziksel Erişim
 - Çalışan biriymiş gibi yapmak
 - Çalışanları arkasından giriş yapmak
 - Postacı, tamirci, misafir, ... gibi davranmak
 - Mesai saatleri dışında girmek
- İlişki Kurmak
 - Sosyal mühendislik yöntemlerini denemek
 - Her çalışma ortamı için uygun ya da yasal olmayabilir.

- Bilgiye Erişim
 - Çalışanları izlemek (omuz sörfü, kulak misafirliği, ...)
 - Ofis içindeki çöpleri karıştırmak, klavyelerin/telefonların/takvimlerin altına, post-it notlarına, panolara göz atmak
 - Ekranı kilitlememiş bilgisayarları kullanmak, kullanıcıları bilgisayarlarını kullanıma açmaya ikna etmek

- Herkesi tanıyan tek bir kişi
- Merkezi güvenlik kayıtları
- Zorunlu geri arama ve geri arama sırasında kontrol
- Anahtar sorular – kullanıcı kayıtlarının doğrulanması
 - Kimlik/personel bilgileri
 - Kişisel soru/yanıtlar (ilk kayıt sırasında belirlenebilir)
- Tuzak sorular
- Hatta bekletmek – hızlı ve hatalı tepki vermemek

- Bir güvenlik sisteminin en zayıf halkası, insan bileşenidir.
- Sosyal mühendislik saldırılarının başarısı, bilgisayar ve ağ sistemlerindeki yerel zayıflıkların gerçekleşme olasılığını artırır.
- Güvenlik politikalarının güncel tutulması, ve personelin uygun bir şekilde bilgilendirilmesi, sosyal mühendislik saldırılarının etkisini azaltmaya yardımcı olur.

