NESNELERİN İNTERNETİ
&
SOSYAL MÜHENDİSLİK

Yrd.Doç.Dr. Muhammed Ali AYDIN
İstanbul Üniversitesi
Bilgisayar Mühendisliği Bölümü
Siber Güvenlik Anabilim Dalı
aydinali@istanbul.edu.tr

NESNELERİN İNTERNETİ

Önemli IoT Güvenlik Açıkları(OWASP)

- Güvensiz Web Arayüzleri
- Hatalı Kimlik Doğrulama/Yetkilendirme
- Güvensiz Ağ Servisleri
- İletişimin Şifresiz İletilmesi
- Hassas Verilerin Gizliliğinin Sağlanamaması
- Güvensiz Bulut Arayüzü
- Güvensiz Mobil Arayüzü
- Yetersiz Güvenlik Yapılandırmaları
- Güvensiz Yazılımlar
- Yetersiz Fiziksel Güvenlik

NESNELERİN İNTERNETİ & GÜVENLİK

- %90'ı Bulut ortamında veya cihazda hassas bilgi barındırıyor!
- %60'ı basit parolaya sahip (İlk kurulumunda yayınlanan ve ayarlanan parolalar)!
- %80'i zayıf parola politikası üzerine kurulu!
- %70'i güvensiz iletişim kuruyor!

NESNELERİN İNTERNETİ & GÜVENLİK

- BotNets
- Hizmet Engelleme (DoS)
- Ortadaki Adam Konsepti
- Veri/Kimlik Hırsızlığı
- Sosyal Mühendislik

Sosyal Mühendislik Nedir?

- Sosyal mühendislik, insanları aldatma sanatıdır.
- Etkileme ve ikna yolu ile insanlardan faydalanmaktır.
- Amaçlanan hedef bellidir.
- İnsan zaafiyeti anahtar nokta!
- Teknolojiyi kullanarak ya da kullanmadan bilgi edinmek için insanlardan faydalanılır.
- İnsanların tanımadıkları biri için yapmayacakları şeyleri yapmalarını sağlama sanatıdır.
- «Beni kimse kandıramaz!» genel yargısı
- Saldırgan, isteğini o kadar akıllıca sunar ki hiç kuşku uyandırmaz ve kurbanın güvenini sömürür.

Sosyal Mühendislik Kavramı

- Genellikle güvenlik gündeme geldiğinde teknik tedbirlerden bahsedilir.
- Bilgi güvenliği sağlanırken insan faktörünün payı teknik önlemlerden çok daha büyüktür!
- Bilinçsiz bir kullanıcının bulunduğu bir ortamda güvenlik sağlamak zordur!
- Kevin Mitnick de bunun farkındaydı.
  - "Sosyal Mühendislik Cephanemdeki En Güçlü Silahlardan Biriydi"
  - "İnsan Unsuru Aslında Güvenliğin En Zayıf Halkasıdır"
  - "Sorun Makinelerde Değil, İnsan Unsurunda"
- Kurbanın merakı, vicdanı, inancı, güveni, acıma duygusu, zaafları(makam, mevki, hırs, para, cinsellik, ego) gibi duyguları kullanılarak gerçekleştirilebilir.

Sosyal Mühendislik Süreci

Sosyal Mühendislik Yöntemleri

- Yöntemler verinin kaynağına, verinin gizliliğine, verinin nasıl korunduğuna göre değişmektedir.
- Temel Sık Kullanılan Yöntemler:
  - Sahte senaryolar uydurmak (pretexting)
  - Güvenilir olduğuna ikna etmek (phishing)
  - Zararlı Yazılımlar (Truva Atları vb.)
  - Güven kazanarak bilgi edinmek
  - Omuz Sörfü
  - Çöpü Karıştırmak
  - Eski Donanımları Karıştırmak

Sahte Senaryolar Uydurmak

- Genellikle telefonla veya bire-bir tarzda gelişen saldırı yöntemidir.
- Hedefin belirlenmesi, hedefe dair bilgi toplanması, hedefle iletişim/ilişki kurulması aşamasından sonra saldırıya geçilir.
- Amaç, sahte bir senaryo/hikaye uydurarak hedeften istenilen bilgiyi almaktır. (kişisel bilgiler, şifreler, özel bir sır vs)
- Saldırı başlangıcında güçlü ve etkili olabilmek için hedefe dair bazı bilgilerin elde edilmesi gerekir.

Güvenilir Olduğuna İkna Etmek

- Oltalama Saldırısı olarak bilinen en etkili saldırı yöntemlerinden biridir.
- Genellikle e-posta üzerinden ilerleyen bir sosyal mühendislik yöntemidir.
- Güvenilir ya da doğruluğu sorgulanamaz bir kaynaktan geldiğine inandırır.
- Saldırganın hedefleri arasında hassas bilgi vermeye zorlamak, ya da kullanıcıyı hatalı bir hareket yapmaya (sahte web sayfasına tıklamak, virüslü yazılım kurmak vb.) yönlendirmektir.

Kullanılan Donanımlar

USB bellekli saat

Donanımsal keylogger

USB bellekli çakmak

Kameralı araba anahtarı

SD kartı saklayıcısı

Kameralı kalem

Kameralı gözlük

Kolay Erişilebilir Bilgi Kaynakları

Sosyal Ağlar

Tehditler

- Yetkisiz Erişim
- İtibar ve Güven Kaybı
- Hassas Bilgiye Erişim ve Veri Kaybı
- Yasal Yaptırıma Uğramak

Örnek Uygulama 1

(Sahte bir senaryo uydurarak telefon ile e-mail şifresi ele geçirme)

- **Kurban(K):**Personel1
- **Saldırgan(S):** Personel2, ben Üniversite Bilgi İşlem'den arıyorum sizin e-mailinizin yabancı kişiler tarafından ele geçirildiğini düşünüyoruz.
- **K:**Nereden anladınız böyle bir şeyi? Ben hiç fark etmedim.
- **S:**Şu an e-mailinizden üniversitemiz güvenlik duvarına saldırılar gerçekleştiriliyor. Bunu önleyebilmemiz için şifrenize ihtiyacımız var.
- **K:**Tamam da ben sizin Bilgi İşlem'den aradığınıza nasıl emin olacağım?

Örnek Uygulama 1

(Sahte bir senaryo uydurarak telefon ile e-mail şifresi ele geçirme)

- **S:** Ben Personel2, şu anda kanıtlayamam tabi ki fakat zamanla yarışıyoruz sizden bu konuda insiyatif almanızı rica edeceğim. Eğer başarılı olamazsak bu konuda sizde sorumlu tutulacaksınız.
- **K:**Bu olay nasıl olmuş benden mi kaynaklanıyor biraz daha bilgi verir misiniz?
- **S:**Kimden kaynaklandığını biz de bilmiyoruz ama olayı çözdükten sonra sizi de bilgilendireceğiz bu konu hakkında ama şu anda zamanla yarışıyoruz bir an önce şifrenize ulaşmalıyız
- **K:**Tamam kardeşim yaz …….

Örnek Uygulama 2

(Sahte bir senaryo uydurarak bir kişinin kartı bilgilerini ele geçirerek alışveriş yapma)

- **Saldırgan(S):**İyi günler ben ABC Bankası'ndan arıyorum Ahmet Bey ile mi görüşüyorum?
- **Kurban(K):**Evet buyurun benim.
- **S:**Harun Bey Para kart uygulamasına geçiyoruz bu yüzden bazı bilgilerinizi teyit etmek istiyoruz. Şimdi size kontrol amaçlı bazı sorular yönelteceğim.
- **K:**Evet dinliyorum.
- **S:**Annenizin kızlık soyadının 2 ve 4. harfi lütfen.

Örnek Uygulama 2

(Sahte bir senaryo uydurarak bir kişinin kartı bilgilerini ele geçirerek alışveriş yapma)

- **K:**Bursa Adana.
- **S:**Teyit ediyorum evet. Kartınızdaki kart numarası para karta kullanılacağı için teyit etmek maksadıyla kart numaranızı söyler misiniz?
- **K:** Bir saniye, xxxxxxxxxxxxxxxxxxx.
- **S:**Teyit ediyorum, kartınızın arkasında bulunan 3 haneli güvenlik kodunu söyler misiniz?
- **K:**xxx.
- **S:**Bilgilerinizi doğrulamak için telefonunuza bir kod gönderdik şimdi o kodu bana söyler misiniz?
- **K:**xxxxxxxxx.

Örnek Uygulama 3

(Mail sunucusundan sorumlu personeli inandırma yolu ile e-mail şifresi alma)

- **Kurbanlar(K):** Sorumlu Bilgi İşlem Personeli ve E-Mail hesabı ele geçirilecek Kullanıcı
- **Saldırgan(S):**Ben …. Numaralı …. adlı öğrenciyim. E-mail şifremi hatırlayamadığım için e-mail hesabımı kullanamıyorum. Rica etsem alabilir miyim?
- *İlgili bilgiler ……. kolay bir şekilde veriliyor.*
- *Ele geçirdiği bu bilgi ile ders kapsamında dersi alan öğrencilere Kurbanın e-mail hesabından mail atılarak oltalama saldırısı düzenleniyor. Bu e-mail bilgisi Kurban tarafından öğreniliyor ve …*
- **K:** Arkadaşlar, Şu an oltalama saldırısı ile karşı karşıyasınız. Sakın benim hesabım diye gönderilmiş mailden gelen dosyaları açmayın. Şu an ciddi bir sosyal mühendislik saldırısı ile karşı karşıyayız. OYUNA GELMEYİN!...

Örnek Uygulama 4

(Anket yapılarak kişilerin e-devlet şifrelerini ele geçirmeye çalışma)

- **Kurbanlar:**E-devlet kullanıcıları
- **Saldırgan:**Anketi düzenleyen kişi/kişiler. Bakırköy meydanda kişiler üzerinde e-devlet kullanımları hakkında bilgi edinmek ve e-devlet şifrelerini kontrol etmek amaçlı anket yapıldığı belirtilerek kişilerin basılı formları doldurulması sağlanmıştır. Formda özellikle alt kısımda «Görevlilerimizden kimliklerini göstermelerini mutlaka isteyiniz.» ibaresi de belirtilmiştir.
- **Sonuç:**Kısa sürede 10 kişi ile anket yapılmış, 2 kişi tüm bilgilerini vermiş. 4 kişi sadece iletişim bilgilerini vermiş. 4 kişi ise hiçbir bilgi vermemiştir. Bilgisi alınan kişiler ise anket sonucunda uyarılmıştır.

Sosyal Mühendislik Saldırılarını Belirlemek ve Durdurmak

- Birisi aşırı derece aciliyet hissi yaratıyorsa, Eğer kendinizi hızlı bir karar verme noktasında buluyorsanız,
- Birisi ulaşmaması gereken ya da zaten önceden bilmesi gereken bir bilgi soruyorsa,
- İnanılmayacak derecede iyi bir şey olmuşsa,

Şüpheci davranın!

- Sosyal Mühendislik saldırılarının nasıl engelleneceğini, durdurulacağını ve nasıl tespit edileceğini öğrenmek kendinizi korumak için uygulayabileceğiniz en etkili adımlardan biridir!

Olası Saldırıları Engellemek

- Şifrelerinizi asla paylaşmayın
- Çok fazla bilgi paylaşmayın
- İrtibatta bulunduğunuz kişileri doğrulayın
- Size sorulan sorulara sorularla karşılık verin

Sosyal Mühendisliğe Karşı

- Kurumun tüm çalışanları bilgi güvenliğinin bir parçası, eğitimler periyodik olarak düzenlenmeli
- Güvenlik politikaları ve prosedürleri
- Verilen eğitimlerin geri dönüşümü
- Çalışanlar ile bilgi güvenliği çerçevesinde gizlilik sözleşmesi
- Kurumun iç sayfasına bilgi güvenliğiyle ilgili görsel tasarımlar, posterler
- Belirli aralıklarla e-mail ile bilgilendirme
- Risk analizi ve bilgi güvenliği testleri yapma

Sosyal Mühendisliğe Karşı

- Güvenlik yazılımlarının güncel tutulması
- Çöpe atılması gereken dokümanların imhası
- Şifre korumalı ekran koruyucular kullanma
- Temiz masa / temiz ekran politikası
- Size özel bilginizi (örneğin şifreniz) kimseyle paylaşmayın.
- Kullanılan şifrelerin her yerde aynı olmaması
- Açık bilgi veritabanlarında bilgilerinizi paylaşmayın
- Denetim
- Sosyal Mayınlar

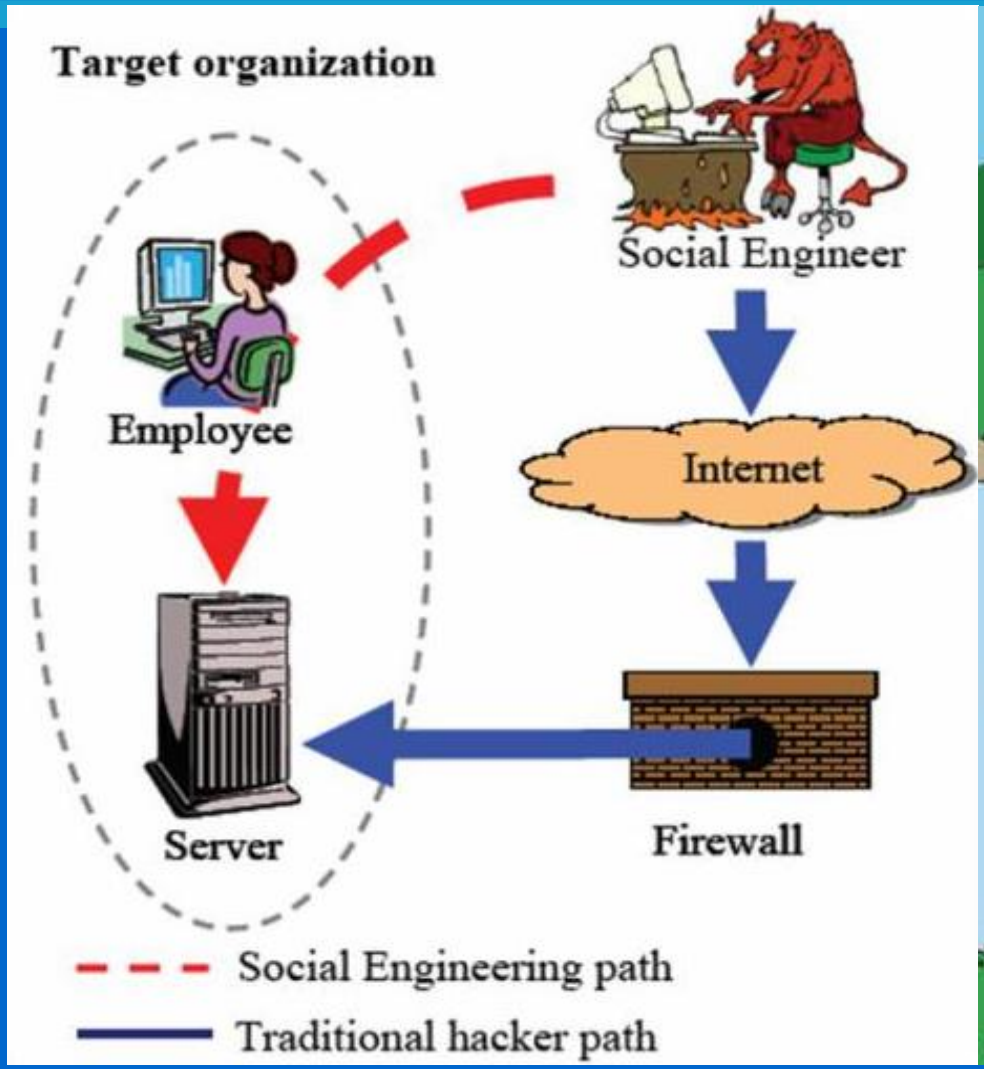
SONUÇ

- Güvenlik ≠ Nesnelerin Akıllanma Hızı

&

- Kullanıcıların IoT Kültürüne Hazırlanması

Sorular


Target organization
Social Engineer
Employee
Internet
Server
Firewall
Social Engineering path
Traditional hacker path


BOĞA İLE BALIK İYİ ANLAŞIR DERLER... GELSENE.
BURÇLARDAN PEK ANLAMAM.
DİKKAT! PİRANHA GÖLÜ
FARUKEN BAYRAKTARE