SOSYAL MÜHENDİSLİK

Tanım:
Bilgi güvenliği bağlamında sosyal mühendislik, gizli bilgileri ifşa etmek için insanların psikolojik olarak manipüle edilmesidir.

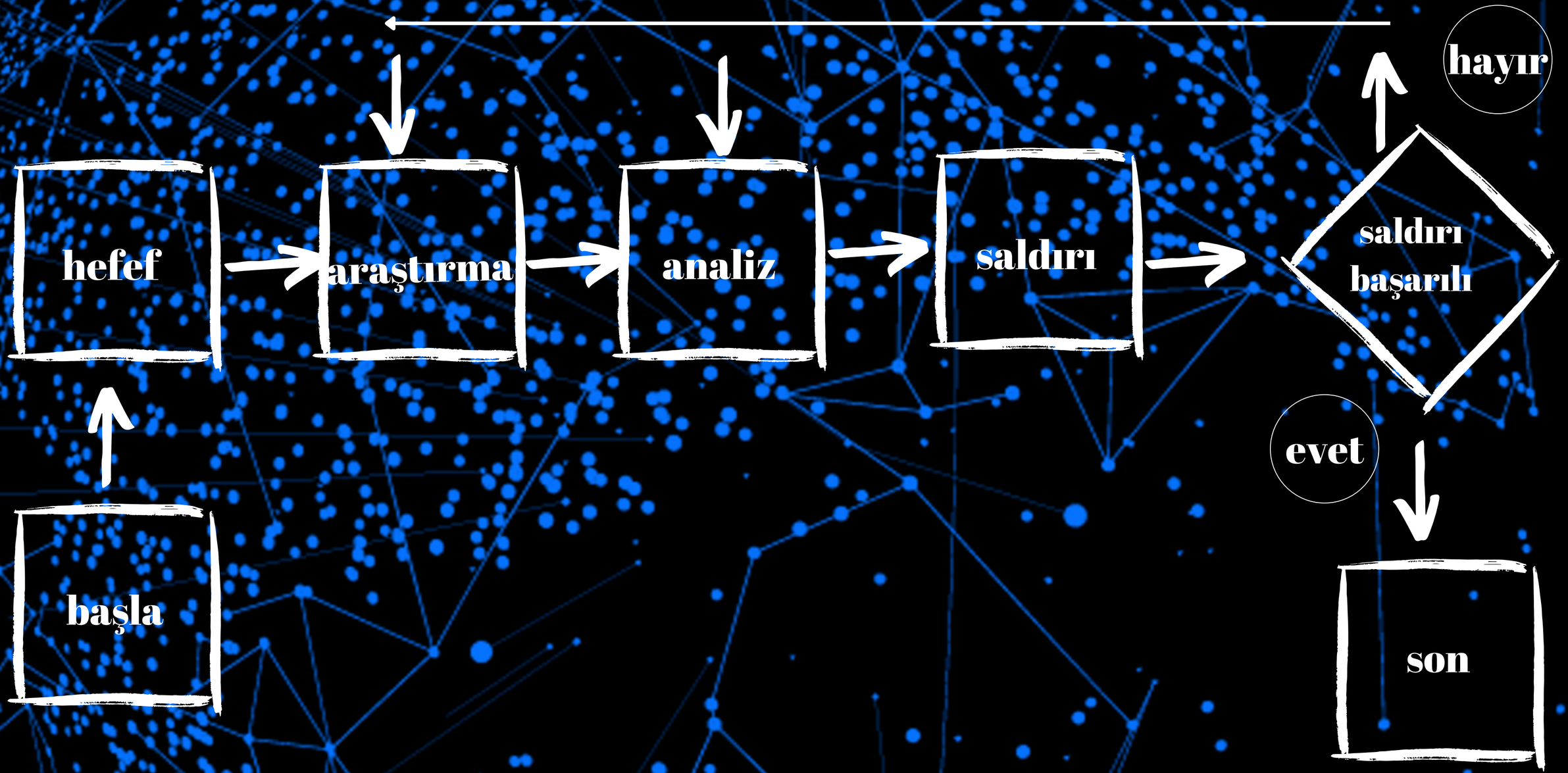
içerik

En zayıf halka insandır

1. Giriş

Bilgi ve bilişim sistemlerinin kullanımı gün geçtikçe artmakta; bu da kötü niyetli kullanıcıların özel bilgilere erişim çabalarının çoğalmasına yol açmaktadır. Bilişim sistemlerini kuran ve kullanan bireyler, güvenlik açıklarını tanıyarak bu açıkları kapatma konusunda bilgi sahibi olurlarsa, hem sistemler korunabilir hem de kullanıcılar tuzaklara düşmez. Sanal ortamda saklanan bilgiler, güvenlik sistemleri ile korunmakta, ancak insan zafiyetleri bu güvenlikleri aşmak için bir fırsat sunmaktadır. Sosyal mühendislik, bu insan zafiyetlerinden faydalanarak veri elde etme sanatıdır. Bu çalışmada, sosyal mühendislik kavramları ve bu saldırılara karşı farkındalığın artırılması için yapılabilecekler incelenmektedir.

işin algoritması



Bilgi güvenliği kültürü

Çalışan davranışları, bilgi güvenliği üzerinde önemli bir etkiye sahiptir. "Örgüt Kültürü ve Bilgi Güvenliği Kültürü Arasındaki İlişkiyi Keşfetmek" çalışması, bilgi güvenliği kültürünü, bilginin korunmasına katkıda bulunan davranış kalıplarının toplamı olarak tanımlamaktadır. Andersson ve Reimers ise, çalışanların genellikle organizasyonun bilgi güvenliği çabasının bir parçası olarak kendilerini görmediklerini ve bu nedenle organizasyonel bilgi güvenliğini göz ardı eden eylemler gerçekleştirdiklerini bulmuşlardır. Araştırmalar, bilgi güvenliği kültürünün sürekli olarak geliştirilmesi gerektiğini göstermekte ve bunu yönetmek için beş adım önerilmektedir: Ön değerlendirme, stratejik planlama, operasyonel planlama, uygulama ve son değerlendirme.

- Ön Değerlendirme : Çalışanlar arasında bilgi güvenliği farkındalığı düzeyini belirlemek ve mevcut güvenlik politikasını analiz etmek.
- Stratejik Planlama: Daha iyi bir farkındalık programı oluşturmak için net hedefler belirlemek.
- Operatif Planlama: İç iletişim, yönetimin katılımı, güvenlik bilinci ve eğitim programına dayalı iyi bir güvenlik kültürü oluşturmak.[5]

Teknikler ve terimler

Tüm sosyal mühendislik teknikleri, insan karar verme süreçindeki bilişsel önyargılara dayanır. Bu önyargılar, çalışanların gizli bilgilerini çalmak için kullanılan çeşitli saldırı teknikleri oluşturur. En yaygın sosyal mühendislik türü telefonla yapılan saldırılardır.

Örneğin, bir kişi resmi görünümlü bir duyuru ile yardım masası numarasının değiştiğini bildirip, çalışanlardan şifrelerini ve kimliklerini istemektedir. Diğer bir örnek ise bilgisayar korsanının sosyal medya aracılığıyla hedefle iletişime geçip, güven kazanarak hassas bilgilere erişim sağlamasıdır.

Sosyal mühendislik, Robert Cialdini'nin oluşturduğu altı ilkeye dayanır: karşılıklılık, bağlılık ve tutarlılık, sosyal kanıt, otorite, sempati ve kıtlık.

İKİ KISMA AYRILIR

Altı temel ilke

Karşı Tedbirler

Altı temel ilke

1. **Karşılıklılık - İnsanlar kendisine yapılan bir iyiliğe karşılık verme eğilimindedir, örneğin pazarlamada ücretsiz örneklerin yaygınlığı bu nedenledir. Cialdini konferanslarında, Etiyopya'nın o sırada felç edici bir kıtlık ve iç savaştan muzdarip olmasına rağmen, 1985 depreminden hemen sonra Meksika'ya binlerce dolar insani yardım sağlaması örneğini sık sık kullanıyor. Etiyopya, İtalya'nın 1935'te Etiyopya'yı işgal ettiği sırada Meksika'nın sağladığı diplomatik desteğe karşılık veriyordu. İyi polis / kötü polis stratejisi de bu prensibe dayanmaktadır.**
2. **Bağlılık ve tutarlılık - İnsanlar bir fikre veya hedefe sözlü veya yazılı olarak taahhüt verirlerse, bu bağlılığı yerine getirme olasılıkları daha yüksektir. Cialdini, Çinliler'in Amerikan savaş esirlerinin kendi imajlarını yeniden yazmak ve otomatik olarak zorlanmadan itaat kazanmak için beyinlerini yıkadıklarına dikkat çekiyor. Diğer bir örnek, pazarlamacıların kullanıcıya pop-up ekranı kapatma sırasında "Daha sonra kaydolurum" veya "Hayır teşekkürler, para kazanmamayı tercih ederim" şeklinde seçenekler sunmalarıdır.**
3. **Sosyal kanıt - İnsanlar, diğer insanların yaptığını gördükleri şeyleri yaparlar. Örneğin, bir deneyde, bir veya daha fazla katılımcı gökyüzüne bakar; daha sonra etrafta bulunanlar neyi kaçırdıklarını görmek için gökyüzüne bakarlar. Bkz:Asch deneyi.**
4. **Otorite - İnsanlar, sakıncalı davranışlarda bulunmaları istense bile otorite figürlerine itaat etme eğiliminde olacaktır. Cialdini, 1960'ların başındaki Milgram deneyleri ve My Lai katliamı gibi olayları örnek verir.**
5. **Sempati - İnsanlar sempati duydukları diğer insanlar tarafından kolayca ikna edilir. Cialdini, Tupperware'in artık viral pazarlama olarak adlandırılabilecek olan pazarlamasından bahsediyor. Satan kişiyi beğenen insanların satın alma olasılıkları daha yüksektir.**
6. **Kıtlık - Algılanan kıtlık talep yaratacaktır. Örneğin, tekliflerin "yalnızca sınırlı bir süre için" mevcut olduğunu söylemek satışları teşvik eder.**

Karşı Tedbirler

Kuruluşlar, güvenlik risklerini şu yollarla azaltır:

Çalışan Eğitimi Çalışanları, konumlarıyla ilgili güvenlik protokolleri konusunda eğitmek.

Standart Çerçeve Çalışan / personel düzeyinde güven çerçeveleri oluşturmak (yani, hassas bilgilerin ne zaman / nerede / neden / nasıl ele alınacağını belirlemek ve personeli eğitmek)

Bilgilerin İncelenmesi Hangi bilgilerin hassas olduğunu belirleme ve sosyal mühendislik ve güvenlik sistemlerindeki arızalara (bina, bilgisayar sistemi vb.) raruz kalma durumunu değerlendirme.

Güvenlik Protokolleri Hassas bilgilerin işlenmesi için güvenlik protokolleri, politikaları ve prosedürleri oluşturma.

Olay Testi Güvenlik çerçevesi için habersiz, periyodik testlerin gerçekleştirilmesi.

Aşılama İlkna girişimlerine benzer veya ilgili girişimlere maruz kalma yoluyla direnç aşılayarak sosyal mühendislik ve diğer hileli hileler veya tuzakları önlemek.[8]

Gözden Geçirme Yukarıdaki adımları düzenli olarak gözden geçirmek: bilgi bütünlüğüne yönelik hiçbir çözüm mükemmel değildir.[9]

Atık Yönetimi Kilitli çöp kutuları bulunan, anahtarları yalnızca atık yönetimi şirketi ve temizlik personeli ile sınırlı bir atık yönetimi hizmeti kullanmak.[10]

SOSYAL MÜHENDİLİĞİN DÖNGÜSÜ

1. **Bilgi toplama, mağdurun alışkanlıklarını çok sabır ve dikkatle izlemeyi gerektiren ilk ve en önemli adımdır.**
2. **Mağdurla ilişki kurma - Gerekli miktarda bilgiyi topladıktan sonra, saldırgan, mağdurla uygun bir şekilde konuşma açar.**
3. **Saldırı -Bu adım genellikle hedefle uzun bir etkileşim süresinden sonra ortaya çıkar ve bu sırada hedeften sosyal mühendislik kullanılarak, aşamalı olarak bilgi alınır.**
4. **Kapanış etkileşimi - Bu, mağdurda herhangi bir şüphe uyandırmadan saldırgan tarafından iletişimin yavaşça kapatılmasını içeren son adımdır. Mağdur saldırı gerçekleştiğini bile nadiren anlar.[11]**

Önleyici tedbirler

Bazı önlemler, sosyal mühendislik dolandırıcılıklarının kurbanı olma riskini azaltır:

- **"Gerçek olamayacak kadar iyi" görünen tekliflerin farkında olmak.**
- **Bilinmeyen kaynaklardan gelen eklere tıklamaktan kaçınmak.**
- **E-posta, telefon veya kısa mesaj yoluyla kimseye kişisel bilgi vermemek.**
- **Spam kutusu gibi spam filtre yazılımlarının kullanılması.**
- **Gerçek hayatta tanınmayan insanlarla sanal ortamda arkadaş olmaktan kaçınmak.**
- **Çocuklara internet üzerinden zorbalığa (siber zorbalık) maruz kalmaları veya çevrimiçi herhangi bir şey tarafından tehdit altında hissetmeleri durumunda güvendikleri bir yetişkinle iletişime geçmelerini öğretmek. [12]**

HAZIRLAYAN : SAMET ŞAHİN

SON