Sosyal Mühendislik: Yaygın Ataklar ve Güvenlik Önlemleri

M. Zekeriya Gündüz
Bingöl Üniversitesi, Teknik Bilimler M.Y.O., Bilgisayar Teknolojileri Bölümü, 12000, Bingöl, Türkiye.
zekeriyagunduz@gmail.com

Resul Daş
Fırat Üniversitesi, Teknoloji Fakültesi, Yazılım Mühendisliği Bölümü, 23119, Elazığ, Türkiye.
rdas@firat.edu.tr

***Özet*—Bilişim sistemlerinde bilgi ve sistem güvenliğinin sağlanması ve verilerin korunması sadece teknolojik çözümlerle mümkün değildir. Çünkü en güvenli sistemlerin arkasında bile bir insanın olduğu dikkate alınmalıdır. Güvenlik zincirindeki en zayıf halka olan insan, farklı zamanlarda farklı davranışlar sergilemesinden dolayı güvenlik sürecinde çeşitli zafiyetler gösterebilmektedir. Bu zafiyetleri ortaya çıkarmak ve istismar etmek sosyal mühendislik kavramının ortaya çıkmasına sebep olmuştur. Bilgi güvenliğinin sağlanması, bilginin korunumuna yönelik teknik ve sosyal boyutun beraber değerlendirilmesi ile mümkün olmaktadır. Bu makale çalışmasında, sosyal mühendislik kavramının toplumda bir farkındalık oluşturması bakımından günümüz güvenlik zafiyetleri örneklerle sunulmuş ve bu zafiyetlerin giderilmesi için çeşitli önlemler ortaya konulmuştur.**

***Anahtar Kelimeler* — Sosyal mühendislik, toplum mühendisliği, bilgi güvenliği, sosyal mühendislik süreçleri.**

***Abstract*—In information systems, provision of information and system security, and also protection of data are not possible with just technological solutions. Because, it should be considered that there is a human even behind the most secure system. The human, who is the weakest link in the security chain, can show various weaknesses in the security process since he reveals different behaviors at different times. To reveal and exploit these weaknesses have led to the emergence of the concept of social engineering. The provision of information security is possible together with the assessment of the technical and social aspects for the protection of information. In this paper, the present security weaknesses have been shown in order that social engineering concept can create awareness in the society, and several precautions have been introduced to resolve these weaknesses.**

***Keywords*—Social engineering, society engineering, information security, social engineering processes.**

I. GİRİŞ

Bilgi ve bilişim sistemlerinin kullanımı günlük yaşamımızda her geçen gün daha fazla hissedilmektedir. Bilişim sistemlerinin kullanıcı sayısı arttıkça bilişim sistemlerinde bulunan açıklardan faydalanarak kullanıcıların özel bilgilerine erişmek isteyen kötü niyetli kullanıcıların sayısındaki artış da açıkça görülmektedir.

Bilişim sistemlerini kuran ve bilişim sistemlerini kullanan bireyler, güvenlik açıkları ve bu açıkları kapatabilmek için gerekli işlemleri bilerek sistemleri kullanır duruma gelirlerse; hem bilişim sistemleri kötü niyetli kullanıcıların saldırısından korunabilecek hem de bilişim sistemlerini kullanan kullanıcılar kötü niyetli kullanıcıların tuzaklarına düşmeyeceklerdir [1, 2].

İş ve sosyal yaşamda bilginin birçok şekli üretilir, değiştirilir, kullanılır, ele alınır ve çeşitli şekillerde iletilir. Sanal âlemin artık bilginin asıl saklandığı depolar haline geldiğini söylemek kaçınılmazdır. Sanal âlemden önce, bilgiler kasalarda, kimselerin bilmediği yerlerde ya da birer sır olarak saklanırdı. Günümüzde ise bu bilgiler genellikle sanal ortamlarda saklanmaktadır. Bu bilgilerin güvenliğinin sağlanması ele alınması gereken ciddi bir mesele olarak insanoğlunun karşısına çıkmaktadır. Kıymetli olan bu bilgilerin istenmeyen kişilerin ellerine geçmesini engellemek için güvenlik sistemleri kullanılır. Teknik anlamda günümüz şartlarında bu güvenlik sistemlerinin aşılmasının imkânsıza yakın olduğunu söylemek mümkündür. Ancak bu sistemlerin aşılması noktasında devreye insan zafiyetleri faktörü girer [3, 4].

En gelişmiş güvenlik sistemlerinin başında bile insan(lar) vardır. Bazı durumlarda bu insan(lar)ın kişisel zafiyetlerinden yararlanılarak sistemlere sızmak daha etkin bir yol olarak görülebilmektedir. Çünkü güvenlik, zincir halkalarının birleşiminden oluşan bir yapı olarak düşünüldüğünde, güvenlik sistemindeki en zayıf halka insandır [5]. Bu zayıf halkanın istismarı ile veri elde etmek sosyal mühendislik (toplum mühendisliği) kavramını ortaya çıkarmıştır. Sosyal mühendislik güvenlikte en zayıf halkanın insan olduğunu kabul eder ve bunun istismarı için çeşitli yöntem ve teknikler kullanır [6].

Sosyal mühendislik için şu tanımlar yapılabilir:
-Hassas/önemli bilgilere ve ağ sistemlerine, yasal kullanıcılar üzerinden erişim sağlama amacıyla saldırganlar tarafından kullanılan düşük teknolojili ve insan zafiyetlerine dayalı yöntemlerin tamamıdır.
- Teknolojiyi kullanarak ya da kullanmadan normal şartlar altında sahip olunamayacak bilgilerin elde edilme sanatıdır [6].
-Normalde insanların tanımadıkları biri için yapmayacakları şeyleri yapmalarını sağlama sanatıdır.
-Teknoloji kullanımından çok, insanların hile ile kandırılarak bilgi elde edilmesi işlemidir.

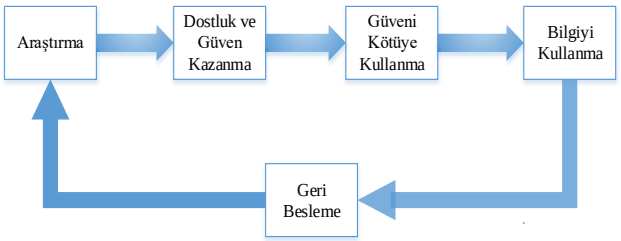
Bu çalışmada sosyal mühendislik ile alakalı kavramlar ve sosyal mühendisliğe karşı farkındalığın artırılmasına yönelik yapılabilecekler örnek olaylar ile aktarılarak, konunun hem bireysel hem de kurumsal düzeyde öneminin anlaşılmasına yönelik değerlendirmeler yapılarak en zayıf halkanın

güçlendirilmesi amacıyla bilgi güvenliği farkındalığının oluşturulması amaçlanmıştır.

II. SOSYAL MÜHENDİSLİK SÜRECİ

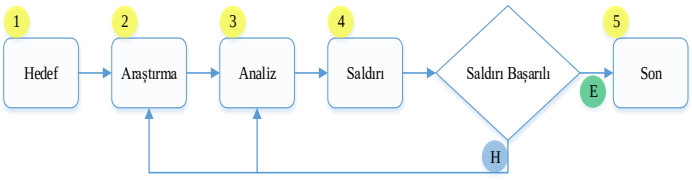
Güvenlik, teknoloji kadar insan ve o insanların teknolojiyi nasıl kullandığı ile ilgilidir. Güvenlik sadece doğru teknolojinin kullanılmasından daha ileride bir hedeftir. Eğer teknolojinin tek başına güvenlik problemini çözebileceği düşünülürse, güvenlik problemi ve güvenlik teknolojileri tam anlaşılmamış demektir [6].

Bilginin korunumuna yönelik bilinmesi gereken bir gerçek de şudur ki; güvenliğin büyük bir yüzdesi kullanıcılara bağlıdır. Dünyanın en gelişmiş güvenlik sistemlerinde bile insan zafiyetlerinden yararlanılarak şifreler ele geçirilirse kullanılan teknik güvenlik etkisiz kalacaktır[7,8]. Bu durum son kullanıcıların sosyal mühendislere karşı her zaman dikkatli olmasını gerektirmektedir. Sosyal mühendisler bazen insanın yanı başındaki en yakın arkadaşları bile olabilmektedir. Sosyal mühendisliğin uygulanmasındaki süreç şekil-1'de gösterildiği gibi sosyal mühendisin kurban hakkında araştırma yapması, kurbana karşı güvenini sağlamak amaçlı hareket, davranış ve eylemlerde bulunması ile istediği bilgiyi elde etmesi olarak görülür. Elde ettiği bu bilgiyi kullanacağı amaç doğrultusunda dener. Başarısız olması durumunda bilgi elde ettiği kurban, yani kaynağa tekrar bağlantı sağlayarak elde ettiği bu bilgileri sosyal mühendislik yöntemleri ile doğrulatabilir. Sosyal mühendislikte veri kaynağına tekrar ulaşabilmek için açık kapı mutlaka bırakılır.



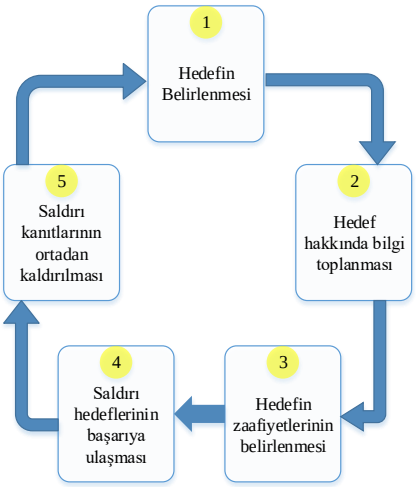
Şekil-1. Sosyal Mühendislik Süreci

Sosyal mühendislik saldırılarının temel düzeydeki saldırı mantığının şematik gösterimi şekil-2 de gösterildiği gibidir. Bir sosyal mühendisin saldırısını başarılı kılmak için tekrar tekrar girişimlerde bulunacağı saldırı akış şemasından anlaşılmaktadır.



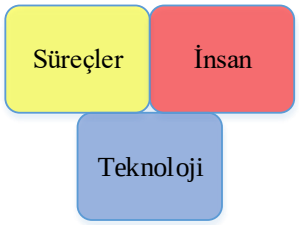
Şekil-2. Sosyal mühendislik saldırısı akış şeması

Bir sosyal mühendislik saldırısının yaşam döngüsü şekil-3'de gösterildiği gibidir. Sosyal mühendisler tarafından her bir basamağın gereklilikleri belli bir düzen içinde yapılmaktadır. Özellikle hedef hakkında can alıcı bilgilerin toplanması ve son adımda sosyal mühendisi ele verebilecek tüm delillerin ortadan kaldırılması sosyal mühendislik yaşam döngüsünün en önemli basamaklarını oluşturmaktadır.



Şekil 3. Sosyal mühendislik saldırısının yaşam döngüsü

Sosyal mühendislik süreci değerlendirildiğinde bilgi güvenliğinin de aslında bir süreç gerektirdiği ve güvenliğin bir ürün değil, bir süreç olduğu anlaşılmaktadır[9,10]. Şekil-4 bilgi güvenliğin sağlanması açısından en önemli üç etkeni göstermektedir. Teknoloji, güvenlik için kullanılan teknik düzeydeki sistem donanım elemanlarını ifade eder. Süreçler ise güvenlik politikalarını ve uyulacak kuralları belirler. İnsan öğesi ise her an farklı duygular taşıyabileceğinden güvenlik temel öğelerinden en değişkeni olarak görülür.



Şekil-4. Bilgi güvenliği sürecindeki öğeler

Sosyal mühendislik sürecinin işlemesinde güvenliğin sağlanması için yapılacak en etkin yöntem en zayıf halka olan insan öğesinin güçlendirilmesi olacaktır. İnsan öğesinin güvenlik farkındalığı arttıkça güvenlik düzeyi de artacaktır. Çünkü en pahalı ve güvenli sistemlerin bile insan zafiyetinden yararlanılarak şifreleri ele geçirildiğinde teknik güvenliğin pek bir anlamı kalmayacaktır [11, 12]. Bilgi güvenliğinin daha etkin olmasını sağlamak için *süreçler, insan ve teknoloji* birlikteliğinin "eğitim" etkeni ile desteklenmesi daha verimli olacak ve bu durum anti-sosyal mühendislik algısını güçlendirecektir.

III. TEMEL KAVRAMLAR ve SALDIRI YÖNTEMLERİ

Sosyal mühendisliğe ait tanımların ve etki düzeyinin bilinmesi, alınması gereken tedbirler ve yapılması gerekenler konusunda bilgi güvenliği açısından farkındalık oluşturacaktır. Bu bağlamda sistem güvenliği dendiğinde işin hep teknik boyutu düşünülür, ancak daha etkili bir güvenlik almak için insan davranışlarına da dikkat etmek gerekmektedir. Faydalı gibi görünüp asıl amacı sisteme sızmak olan truva atının (trojan) sosyal mühendisliğin bir ürünü olduğunu söylemek mümkündür. Askeri bir zafer olarak bilinen troy (truva) efsanesinde bile teknik bir zaferden ziyade davranışsal bir zafer vardır. Bir sistem dünyanın en iyi güvenlik sistemlerine sahip olabilir, ancak insan davranışları bu sistemlerin güvenlik düzeylerini belirler. Bu yüzden sosyal mühendislik davranışlarına karşı önlemler alınmadığında en güvenli sistemlerin bile aşılması mümkündür. Bununla beraber sosyal mühendislik saldırılarına teknolojik bir unsur eklendiğinde daha tehlikeli bir hal almaktadır. Çoğu insan, kandırılma olasılığının çok düşük olduğunu düşünür. Bu ortak inancın bilincinde olan saldırgan, isteğini o kadar akıllıca sunar ki hiç kuşku uyandırmaz ve kurbanın güvenini sömürür. Sosyal mühendislik ile alakalı kavramları ve yöntemleri bilmek tedbirli olmak bakımından büyük artılar sağlar [6,13,14].

A. *Sosyal mühendislik kavramları*

Literatürde çoğunlukla bahsi geçen sosyal mühendislik kavramlarından bazıları aşağıda belirtilmektedir [6, 8, 11, 14-18]:

Omuz Sörfü - Omuz Gezintisi (Shoulder Surfing): Klavye ile bilgi giren birinin parolasını ya da başka kullanıcı bilgilerini görüp çalmak amacıyla seyretmektir.

Ters Toplum Mühendisliği (Reverse Social Engineering): Kurbanın bir sorunla karşılaştığı ve yardım için saldırganı aradığı şeklinde gelişen toplum mühendisliği sürecidir.

Çöp Dalışı (Dumpster Diving): İşe yarar bilgiler elde etmek için hedefin çöpünü habersizce karıştırma işidir.

Kimlik Hırsızlığı (İdentity Theft): Bir başkasına ait kişisel bilgilerin başkaları tarafından yetkisiz olarak kullanılması suretiyle işlenen dolandırıcılık yöntemidir.

Oltalama – Sazan Avlama (Phishing): Hassas verileri ele geçirmek için gerçek sistem kimliğine bürünerek sahte e-posta, sohbet(chat) ya da web sitelerinin tasarlanarak kurbanın e-posta adresine link olarak gönderilmesidir. Bir bankadan ya da iyi bilinen bir kurumdan kullanıcı bilgilerinin teyit edilmesi amaçlı bir e-posta gönderilerek yapılır. Bu sahte siteler orijinal sitelerin kopyası şeklinde olup tüm yasal haklara sahipmiş izlenimini verecek şekilde toparlanırlar.

Telefon oltalaması (Vishing): Voice phishing kelimelerinden türetilen Vishing aslında bir phishing türü olup, kurbana gönderilen e-postada bulunan sahte link yerine bir telefon numarasının belirtilmesi ve bu numaranın aranarak bilgilerin güncelleştirilmesi amaçlanır. Böylece kurbanın bilgileri ele geçirilir.

*Kimliğe bürünme (İmpersonation):*Sosyal mühendisin bir kurumda çalışan bir işçi ya da sistem üzerinde yetkilere sahip kullanıcı gibi davranmasıdır. Sosyal mühendis bir kapıcı, işçi ya da taşeron gibi davranarak ortama fiziksel erişim sağlayabilir.

Online Dolandırıcılık (Online Fraud): İçerisinde zararlı yazılım eki bulunan e-posta sosyal mühendis tarafından yollanır. Ekteki bu zararlı yazılımlar şifreyi yakalamak için klavye dinleme yazılımı (keylogger), virüs, truva atı ya da solucanlar olabilir.

Yardım Masası (Help Desk): Klasik sosyal mühendislik tekniklerinden olup, kurban olarak seçilen kişinin teknik olarak yardım etmek amaçlı arandığı ve verilecek talimatları bilgisayarında gerçekleştirmesi amaçlanır.

Önemli bir kullanıcı gibi davranmak (Important User): Sosyal mühendisin bilgisayar sistemine ve dosyalarına erişim hakkı olan *VIP (very important person)* ya da yüksek seviyeli bir yönetici gibi davranmasıdır. Alt kademede çalışan kişiler(işçiler) çoğu zaman bu pozisyonda görülen kişilere soru sormadan dediklerini yaparlar.

Üçüncü Taraf Olmak (Third-party Authorization): Sosyal mühendisin bilgisayar sistemine erişim sağlamak için yetkili bir kişiden izin almış gibi davranarak karşı tarafı inandırmasıdır. Bu yöntem genellikle yetkili kişiye ulaşılamayacağı zaman kullanılır.

Kaynağı Kurutmak: Bir sosyal mühendisin gerçekleştirdiği saldırıyı kurbanın anlamasıdır.

Sosyal Mühendis(Toplum Mühendisi): İnsan davranışlarındaki zafiyetlerden yola çıkarak kişi, kurum veya kuruluş hakkındaki özel veya tüzel bilgilerin izinsizce elde edilmesini sağlayan kötü niyetli kişidir. Sosyal mühendisler bazı kaynaklarda toplum mühendisi olarak da adlandırılmaktadır [6]. Toplum mühendisleri uygulamalarında temelde aldatma unsurunu kullanırlar.

Sosyal mühendislerin belirgin özelliklerinden bazıları şu şekildedir:

- Genellikle telefon ve interneti iyi kullanırlar.
- Yardımsever görünürler.
- Genellikle iyi giyinimli kişilerdir.
- İnsanların güvenini kazanma eğilimi sergilerler.
- Sıradan insanların açgözlülük, korku, ahlaki zorunluluk, şehvet, suçluluk duygusu gibi zayıf yanlarını sömürürler.
- Özenle hazırlanmış bir plan çerçevesinde çalışırlar.
- Söz söyleme sanatı konusunda başarılıdırlar.
- İkna kabiliyetleri yüksektir.
- Etkileyici, nazik ve sempatik kişilik sergilerler.
- Yalan söylemek konusunda çekinceleri yoktur ve bunu karşılarındakine belli etmeden ustalıkla yaparlar.
- Bulundukları ortama göze batmadan uyum sağlayabilirler
- Masum soruların arasına anahtar soruları katma konusunda ustadırlar.
- Acındırma, suçluluk duyurma ve sindirme en çok kullandıkları üç psikolojik yöntemdir.
- Sosyal mühendisler teknik bilgi olarak donanımlı kişiler olmak zorunda değildirler.
- Bir siber saldırgan az veya çok mutlaka sosyal mühendislik yeteneklerine sahiptir.

B. *Sosyal mühendislik Saldırı Yöntemleri*

Sosyal mühendislik saldırıları, verileri ele geçirmek veya açığa çıkarmak, özel veya tüzel bilgileri silmek veya değiştirmek, bilgi güvenliği zafiyetleri doğurarak ilgili kişi ya da kurumların itibarını zedelemek ve iş yaşamında saygınlık kaybına sebep olmak, e-postalar aracılığı ile sistemlere zararlı yazılımlar yükleyerek bilgi almak ya da göndermek, teknik olarak aşılması mümkün olmayan sistemlerin insanların bireysel zafiyetleri ile aşılabileceğini göstermek amaçlı yapılabilmektedir[12].

Günümüz teknolojileri düşünüldüğünde karşılıklı etkileşim açısından sosyal mühendislik türlerini şu iki başlık altında toplamak mümkündür:

1) *İnsan Tabanlı (Human-Based):* İnsan tabanlı sosyal mühendislikte insanlarla doğrudan bire bir etkileşim (person-to-person interaction) vardır. Burada amaç istenen bilginin doğrudan elde edilmesidir. Sosyal mühendisler insan tabanlı sosyal mühendislik tekniklerini farklı şekillerde kullanırlar. Kullanılan en bilindik yöntemleri şunlardır:

- Kimliğe bürünme
- Önemli bir kullanıcı gibi davranmak
- Üçüncü taraf olmak
- Yardım masası
- Omuz sörfü
- Çöp Dalışı
- Vishing

2) *Bilgisayar Tabanlı (Computer-Based):* İstenen bilginin elde edilmesi için bilgisayar yazılımlarının kullanıldığı sosyal mühendislik türüdür. Burada kurban ile doğrudan iletişim yoktur. Sosyal mühendisler bilgisayar tabanlı sosyal mühendislik tekniklerini farklı şekillerde kullanırlar. Kullanılan en bilindik yöntemleri şunlardır:

- Sazan avlama
- Online dolandırıcılık

Kullanılan araçlar bakımından değerlendirildiğinde *telefon sistemlerinin* sosyal mühendisler için vazgeçilmez bir unsur olduğunu söylemek mümkündür. Bu yüzden *telefon tabanlı sosyal mühendislik* ayrı bir başlık altında değerlendirilebileceği gibi birebir etkileşimle gerçekleştiği için birinci grup sosyal mühendislik türüne de girebilir.

Sosyal mühendislik yöntemlerinden en sık kullanılanları şu şekildedir:

- Sahte senaryolar uydurmak
- Karşı tarafı güvenilir bir kaynak olduğuna ikna etmek
- Phishing saldırıları
- Vishing saldırıları
- Güvenilir bilgi karşılığında para, hediye, vs önermek
- Güven kazanarak bilgi edinmek
- Etkileme ile bilgi edinmek
- İkna etme ile bilgi edinmek
- İnandırma ile bilgi edinmek
- Omuz sörfü
- Çöp karıştırmak
- Eski donanımları kurcalamak
- Korkutarak bilgi veya para talep etmek
- Yardımseverlik duygusundan yararlanarak bağış talep etmek
- Bir çalışanın bilgilerini ele geçirerek sisteme sızmak veya güvenliği aşmak.
- Trojan zararlı yazılımları ile bilgi toplamak
- Üst düzey yetkili gibi davranmak
- Kendini acındırmak
- Yardıma ihtiyacı olan bir personel gibi davranmak
- Kurumun herhangi bir bölümündeki çalışan gibi davranmak
- Personele içinde zararlı yazılım bulunan bir flash bellek hediye etmek
- Kurbanı zararlı yazılım barındıran bedava bir programı bilgisayarına kurmasına ikna etmek
- Güven kazanmak için şirket içi terimler kullanmak
- Kurbanı önceden tanıyor gibi konuşmak
- Karşı cinsi etkilemeye çalışmak
- Kendini emniyet, istihbarat personeli gibi tanıtmak
- Teknik destek için aradığını ve talimatlarının aynen yapılması gerektiğine inandırmak.

Sosyal mühendislerin en sık kullandıkları bu yöntemlerden bir veya daha fazlası kurbanın özelliğine göre sosyal mühendis tarafından kullanılır.

IV. BAZI SOSYAL MÜHENDİSLİK ÖRNEKLEMLERİ

Sosyal mühendislerin, kullandığı sosyal mühendislik davranış ve yöntemleri önceki bölümlerde belirtilmiştir. Bu kişilerin, özellikle günümüzde birçok kişinin mağduriyetine sebep olan ve kendilerini bir firmanın yetkili kişisi, savcı, polis, komiser vs. gibi tanıtıp insanları avladıkları artık çok aşikârdır. Bu tür olayları neredeyse her gün haber kanallarından takip etmek mümkündür. Örneğin internet üzerinden yapılan araba satışlarında sosyal mühendislik yöntemleri kullanılarak insanların dolandırıldığı olaylar azımsanmayacak ölçüdedir. Araba satışını yapacak kişinin alıcıya kaparo amaçlı "şu kadar parayı şu hesaba veya isme gönderin" deyip parayı aldıktan sonra kayıplara karışması sık kullanılan yöntemlerdendir.

Aşağıda, iletişim yoluyla, önceki bölümlerde belirtilen sosyal mühendislik yöntemlerinden bazılarının beraber kullanılması ile meydana gelmiş güncel bazı sosyal mühendislik vakaları incelendiğinde sosyal mühendislerin futbolcudan, akademisyene hatta emniyet personeline kadar her kesimden insanı dolandırabilecekleri görülmektedir.

- İnternetten araç satımı gerçekleştiren bir vatandaşın dolandırılması [19].
- Kendini savcı, hâkim olarak tanıtan kişiler tarafından yapılan dolandırıcılık [20].
- Kendisini baş komiser olarak tanıtan kişiler tarafından yapılan dolandırıcılık [21].

- Kendisini il valisi olarak tanıtıp belli miktarda yardım talebinde bulunan kişinin dolandırıcılığı [22].
- Kendisini polis olarak tanıtarak 11 yaşındaki çocuğu dolandırmaya çalışan kişinin yaptığı dolandırıcılık [23, 24].
- Kendisini polis olarak tanıtarak yetişkin bir insanı dolandırmaya çalışan kişinin yaptığı dolandırıcılık [25].
- Sosyal mühendislik yöntemlerini kullanarak telefon dolandırıcılığını ekmek kapısı haline getiren dolandırıcıların kurdukları çağrı merkezi sistemleri ile yaptıkları dolandırıcılıklar [26, 27].
- İnternet bankacılığı için kullanılan telefon numarasının sosyal mühendis tarafından değiştirilmesi ile yapılan online dolandırıcılık [28].
- On beş gün gibi kısa süreliğine kurulan oto galeriler ile yapılan dolandırıcılıklar [29].
- Bu makale çalışması için bazı insanların bilgi güvenliği farkındalık düzeyleri üzerinde yapılan denemelerde, bilmedikleri birisine ait dizüstü bilgisayardan (keylogger programı yüklenmiş) facebook hesaplarına girmeleri istenmiş, sosyal mühendislik teknikleri ile istenen bu isteğe kişilerin hepsinden olumlu cevap alınmış ve hepsinin facebook şifreleri kolaylıkla elde edilmiştir.
- Türkiye'de sosyal mühendislik yöntemleri kullanılarak özellikle telefon üzerinden 2015 yılında 40 milyon TL civarında kayda geçen telefon dolandırıcılığı yapıldığı belirtilmiştir [30].

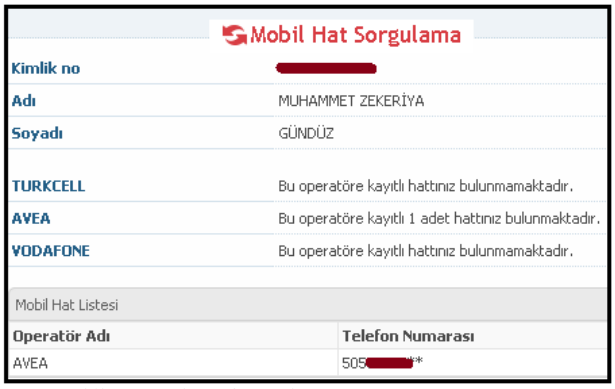
Kayda geçmeyen örneklerin bunlardan kat kat daha fazla olduğu göz önüne alınırsa sosyal mühendislik saldırılarına karşı alınması gereken önlemler açısından toplum üzerinde bilinçlendirme çalışmalarının daha sık yapılması net bir şekilde anlaşılmaktadır. Bu bağlamda gündemdeki mevcut sosyal mühendislik vakalarının bilinmesi sosyal mühendislere karşı tedbirli olmak açısından etkili bir savunma yöntemi olacaktır.

V. TEMEL GÜVENLİK ÖNLEMLERİ

Sosyal mühendislerin kullanmış olduğu yöntem ve tekniklere karşı hem bireysel hem de kurumsal olarak alınabilecek önlemlerden bazıları şu şekilde belirlenebilir:

- Çöpe atılan belge veya dokümanlar, kırpıcılardan geçirilmeli veya okunamayacak şekilde yırtılmalıdır.
- Şifre korumalı ekran koruyucular kullanılmalıdır.
- Kişisel şifreler kesinlikle bir başkasına söylenmemelidir.
- Temiz masa / temiz ekran politikası uygulanmalıdır.
- Bir kurum için işten ayrılan çalışanlar için uyulması gereken prosedürler hazırlanmalıdır.
- Bir kurum için işten ayrılan personellerin kullandıkları sistem parolaları hemen pasif hale getirilmelidir.
- Kuruma ziyaretçi olarak gelen kişilerden kimlik alınmalı, gerekirse kurum içerisinden bir çalışan bu kişiye refakat etmelidir.
- Kişiye özel bilgiler (şifre, kredi kartı numarası gibi) kimseyle paylaşılmamalıdır.
- En yakın kişilerin bile bazen sosyal mühendislik teknikleri ile birbirlerini avlayabilecekleri unutulmamalıdır.
- Bilgi güvenliği için birden fazla e-posta kullanmanın bazı durumlarda daha etkili olabileceği bilinmelidir.
- Hassas kişisel bilgilerin(TC kimlik numarası, telefon numarası, doğum yeri, doğum tarihi vb.) her yerde, özellikle sosyal medyada (facebook, twitter vb.) paylaşılmamasına dikkat edilmelidir.
- İnternette verilen tüm kişisel bilgilere ve paylaşımlara birilerinin ulaştığını bilerek kontrollü hareket edilmelidir.
- Sosyal mühendisliğe karşı alınabilecek en etkin yolun human-firewall (insan güvenlik duvarı), yani kendi yaşamında davranışlarıyla uygulayacağı güvenlik duvarı olduğu bilinmelidir.
- Şifrelerin kâğıtlar üzerine yazılarak görülebilecek yerlere asılmaması konusunda dikkatli olunmalıdır.
- Klavye türü giriş birimlerinden şifre girilirken, giriş yapan kişinin fark etmeyeceği şekilde gözetlenmesi anlamına gelen omuz sörfü yapanlara karşı dikkatli olunmalıdır.
- Özellikle telefonda, her hangi bir istekte bulunan kişinin sesi tanınmıyor ve istemek için herhangi bir nedeni yok ise hiç kimseye kişisel ve kredi kartı bilgileri verilmemelidir.
- Biraz şüpheciliğin toplum mühendislerinin kurbanı olmayı engelleyebileceği bilinmelidir.
- Toplum mühendislerinin yardım talebini çok kullandıkları bilinmelidir.
- Kurumlar için hassas bölgelere 24 saat aktif olan güvenlik kameraları yerleştirilmelidir.
- Tanımadık kişilerden gelen isteklere karşı her zaman temkinli davranılmalıdır.
- Kurumdaki tüm personele periyodik olarak bilgi güvenliği bilinçlendirme eğitimleri verilmelidir.
- Bu çalışmada belirtilen ve yakın zamanda meydana gelen sosyal mühendislik saldırıları ile ilgili vakaların takip edilmesi farkındalığı artırmak ve yeni çıkan sosyal mühendislik yöntemlerini bilmek için etkilidir.
- Periyodik olarak, sosyal mühendislik saldırı testini de içeren, bilgi güvenliği testleri gerçekleştirilmeli ve bilişim teknolojilerinde sisteme en çok zarar verecek kişinin ne yaptığını bilmeyen kişi olduğu bilinmelidir.
- Sosyal mühendislik konusunda farkındalığın artırtılması için sosyal mühendislik içerikli olan Catch me if you can(Sıkıysa Yakala), Who am I(Ben Kimim), Plastic gibi güncel filmler izlenebilir/izletilebilir.
- Telefonda kendisini polis, savcı, asker vb. şeklinde tanıtıp bankaya para yatırılması gerektiğini veya söyleyecekleri yere altın, para bırakılmasının istendiği bir telefon araması ile karşı karşıya kalındığında 155 polis hattı aranarak durum bildirilmelidir. Mümkünse toplum mühendisinin tekrar araması sağlanıp polis ile koordineli şekilde çalışılarak kişinin yargıya teslimi sağlanmalıdır.
- Kişisel bilgileri ele geçiren sosyal mühendislerin habersizce tanımadıkları kişiler adına telefon hatları çıkarması mümkündür telefon kullanımının kontrolünün sağlanması için operatörlere ait sitelerden çevrimiçi kontroller yapılabileceği gibi e-devlet şifresi ile kişilerin

üzerlerinde kayıtlı bulunan telefon numaralarını şekil-5'de görüldüğü gibi takip edebilmeleri de mümkündür.



Şekil-5. Kayıtlı telefon hatların e-devlet üzerinden tespiti

Truva atlarının, zararlı yazılımların ilerlemesinde ve bilgisayara yerleştirilmesinde en fazla kullanılan zararlı yazılım türlerinden olup, genellikle kullanıcı zafiyetlerinden yararlanılarak sosyal mühendisler tarafından sisteme yüklenmesi amaçlandığı son kullanıcılarca bilinmeli ve kaynağından emin olunmayan ve kimden geldiği bilinmeyen e-postalar açılmamalıdır. Özellikle e-posta ile herhangi bir bağlantıya ya da butona tıklatılması, e-postanın yanıtlanması, bilgi girilmesi ya da e-postanın başka bir adrese gönderilmesi, belirtilen telefon numarasının kişisel bilgileri güncelleştirme için aranması, bir programın yüklenmesi vb. herhangi bir eylemin yapılması isteniliyorsa, bu e-postaların güvenlik riski en yüksek saldırılardan olduğu bilinmelidir. Ayrıca içerisinde sosyal mühendislik yöntemleri barındıran phishing e-postaları detaylı incelendiğinde [31];

- Net olmayan ifadelerin kullanıldığı,
- Bazen gereksiz ve alakasız vaatlerde bulunulduğu,
- Bu e-postalarda dil kurallarının(gramer) acemice kullanıldığı,
- Genel ifadeler kullanıldığı,
- Olayın çok acil olduğuna dair kişiyi paniğe sokacak ifadeler kullanıldığı,
- Kişinin verilen talimatları hemen yerine getirmek için harekete geçmesi gerektiği,
- Kişinin önceden bilmediği linklere yönlendirilmesinin amaçlandığı açıkça görülmekte olup bu tür e-postalara karşı dikkatli olunmalıdır.

Bu güvenlik önlemleri sosyal mühendislere karşı belli oranda güvence sağlayabilir. Bunlarla beraber sosyal mühendislerin hedefe ulaşmak için her türlü insani duyguları istismar edebileceği ve her yolu mubah görebileceği unutulmamalıdır. Ayrıca polis teşkilatının ve özellikle bankacılık hizmeti veren kuruluşların son kullanıcıları hem sanal ortamda hem de cep telefonlarına gönderilen kısa mesajlar aracılığı ile sosyal mühendislere karşı dikkatli olmaları noktasında uyardığı ve hatta bununla ilgili bilinç düzeyini artırmak için görsel materyaller bile hazırladıkları bilinmelidir [32]. Sosyal mühendislerin insanları dolandıracakken, kullandıkları yöntemler ile kendi tuzaklarına düştükleri olaylar bazen sosyal medya ve haber kanallarında duyulmaktadır [33, 34].

VI. SONUÇ VE ÖNERİLER

İnsanlar paraları ya da malları çalındığında bunu hemen fark edebilirler ancak bilgileri çalındığında çoğu zaman bunu iş işten geçtikten sonra fark ederler. Teknolojinin bugünkü seviyesinde, yakın birinden gelen bir e-postanın bile güvenli olup olmayacağını düşünüyor olmak yaşamın üzücü bir gerçeğidir. Bu bağlamda bilgi varlıklarını, kişisel bilgileri ve bir kuruma ait hassas alt yapıları korumak konusunda bireyler bilinçli ve eğitimli olmak durumundadırlar. En etkili savunma, bireysel ya da kurumsal düzeyde temel güvenlik politikalarının bilinmesi ve başkalarının kötü niyetli davranışlarının insanları etkileyebileceğinin farkında olunmasıdır. Dünyadaki herhangi bir bilgisayar sistemini kullanan en az bir insan vardır. Bu yüzden eğer saldırgan, sistemleri kullanan insanları etkileyebilirse, sistemin gizliliği anlamsız olacaktır. İnsanlar toplum mühendisliği saldırılarını fark edecek şekilde eğitilmediği ve yetiştirilmediği sürece mağdur insanların sayısında bir azalma olacağını söylemek mümkün değildir. Dolayısıyla dünyada toplum mühendisliği saldırılarını engelleyebilecek bir teknoloji henüz yoktur ancak sürekli bir bilinçlilik bunu engelleyebilecek en etkili silah olacaktır.

Yapılan araştırmalar sosyal mühendislik yöntemlerinin ya doğrudan ya da dolaylı olarak siber suç dünyasında saldırganlar tarafından büyük oranda kullanıldığını göstermektedir. Bu çalışmanın hazırlanması aşamasında yapılan araştırmalarda son kullanıcıların çoğunun sosyal mühendislik saldırısına uğradığının farkında bile olmadıkları görülmektedir. Sosyal mühendislik yöntemlerinin saldırılar içerisinde yoğun kullanılmasının başlıca nedenleri; ağ sistemleriyle alakalı olarak çok fazla teknik bilgi gerektirmeden kullanılabilmesi ve saldırganları sonuca daha çabuk ulaştırabilmesidir.

Sonuç olarak yapılan araştırmalar ışığında ve bu çalışmada verilen örneklerde de görüldüğü üzere, sosyal mühendisliğin kötü niyetli kişiler tarafından yoğun şekilde kullanıldığı ve sürekli yöntemleri değiştirerek başarı göstermektedirler. Bu sebeple, güncel sosyal mühendislik saldırılarına karşı bireylerin bilinçlendirilmesi için ilgili kurum ve kuruluşlar tarafından sürekli bilgilendirmeler yapılmalıdır.

KAYNAKLAR

[1] Gündüz, M.Z., 2013. "Bilişim Suçlarına Yönelik IP Tabanlı Delil Tespiti", Yüksek Lisans Tezi, Fırat Üniversitesi Fen Bilimleri Enstitüsü, Elazığ.

[2] Şenol, A., Karacan, H., "Sazan Avlama(Phishing):Kullanılan Teknikler ve Bunlardan Korunma Yöntemleri", 5. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (5th International Conference on Information Security and Cryptology), 17-18 Mayıs 2012, Odtü, Ankara.

[3] Vural, Y., Sağıroğlu, Ş., "Kurumsal Bilgi Güvenliğinde Güvenlik Testleri ve Öneriler", Gazi Üniv. Müh.Mim.Fak.Dergisi, 26(1), pp. 89-103, 2011.

[4] Karadoğan, İ., Daş, R., Baykara, M., "Scapy ile Ağ Paket Manipülasyonu", 1st International Symposium on Digital Forensics and Security (1. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu), 20-21 Mayıs 2013, Elazığ, Turkey.

[5] Canbek, G., Klavye Dinleme ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme, Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Ankara, 2005.
[6] Mitnick, K.D., Simon, W.L., 2013. "Aldatma Sanatı", Odtü Yayıncılık, Ankara.
[7] Arslan, M., Bal, I., "İnternet Ortamında Karşılaşılan Olası Tehditlere Karşı Üniversite Öğrencilerinin Farkındalık Düzeyinin Ölçülmesi", 1st International Symposium on Digital Forensics and Security (1. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu), 20-21 Mayıs 2013, Elazığ, Turkey.
[8] Karabacak, T., Dal, S., "Siber Tehdidin Tehlikeli Araçlarından Birisi:Sosyal Mühendislik", 7. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (7th International Conference on Information Security and Cryptology), 17-18 Ekim 2014, İTÜ, İstanbul.
[9] Sağıroğlu, Ş., Bulut , H., "Mobil Ortamlarda Bilgi ve Haberleşme Güvenliği Üzerine Bir İnceleme", Gazi Üniv. Müh. Mim. Fak. Dergisi, Cilt 24, No: 3, 499-507, 2009.
[10] Küçüksille, E.U., Yalçınkaya, M.A.,Uçar,O., "Siber Saldırılarda İstismar Kitlerinin Kullanımı Üzerine Bir Analiz ve Savunma Önerileri", 7. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (7th International Conference on Information Security and Cryptology), 17-18 Ekim 2014, İTÜ, İstanbul.
[11] Abraham, S., Chengalur-Smith,I.,"An overview of social engineering malware:Trends, tactics and implications",Technology in Society V. 32, pp.183-196, 2010.
[12] Mouton, F., Malan, M.M., Leenen,L., Venter, H.S., "Social engineering Attack Framework", Information Security for South Africa,13-14 Ağustos 2014, Güney Afrika.
[13] Lee, D.H., Choi, K.H., and Kim, K.J. 2007. "Intelligence Report and the Analysis against the Phishing Attack Which Uses a Social Engineering Technique," Proceedings of the 2007 international conference on Computational science and Its applications 2.
[14] İnternet: http://e-bergi.com/y/Toplum-Muhendisligi, Erişim Tarihi:02.04.2016
[15] Krombholz, K., Hobel, H., Huber, M., Weippl, E., "Advanced Social Engineering Attacks", Journal of Information Security and Applications V.22, pp. 113-122, 2015.
[16] F. Mohd Foozy, R. Ahmad, M. Abdollah, R. Yusof, and M. Mas'ud, "Generic taxonomy of social engineering attack," in Malaysian Technical Universities International Conference on Engineering & Technology, Batu Pahat, Johor, November 2011.
[17] İnternet: https://www.olympos.net/belgeler/phishing/vishing-ile-tanisma-zamani-49491.html, Erişim Tarihi:02.05.2016
[18] İnternet: http://www.bilgiguvenligi.gov.tr/sosyal-muhendislik/sosyal-muhendislik-saldirilari-3.html, Erişim Tarihi:02.05.2016
[19] Kaya, A. ve arkadaşları "Organize Suç Örgütü Tarafından Değişik Bir Yöntem Kullanılarak Yapılan Otomobil Dolandırıcılığı", 1st International Symposium on Digital Forensics and Security (1. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu), 20-21 Mayıs 2013, Elazığ, Turkey.
[20] Kaya, A. ve arkadaşları "Türkiye Genelinde Bilişim Yolu ile İşlenen Dolandırıcılık Suçu:16 Olgu", 1st International Symposium on Digital Forensics and Security (1. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu), 20-21 Mayıs 2013, Elazığ, Turkey.
[21] *İnternet:* http://www.sabah.com.tr/yasam/2014/11/06/rektor-yardimcisini-da-telefonda-dolandirdilar, Erişim Tarihi:22.05.2016
[22] *İnternet:* http://www.aksam.com.tr/sporgalatasaray/burak-yilmaz-dolandirildi/haber-265081, Erişim Tarihi: 22.05.2016
[23] *İnternet:* http://www.haber7.com/elazig/1805716-cocugu-telefonda-dolandirmaya-calisirken-yakalandi, Erişim Tarihi:22.05.2016
[24] *İnternet:* http://video.haber7.com/video-galeri/66582-telefon-dolandiricisi-sucustu-yakalandi, Erişim Tarihi:23.02.2016
[25] *İnternet:* http://www.hurriyet.com.tr/saglik/25019037.asp, Erişim Tarihi:22.05.2016
[26] *İnternet:* http://www.kupurhaber.com/haber/1151/dolandiricilik-icin-cagri-merkezi-kuran-ceteye-siber-baskin.html, Erişim Tarihi:23.05.2016
[27] *İnternet:* http://www.sabah.com.tr/yasam/2016/01/27/cagri-merkezi-ile-dolandiricilik-operasyonu-40-gozalti, Erişim Tarihi:23.05.2016
[28] *İnternet:* http://www.internethaber.com/akilalmaz-sanal-dolandiricilik-150405h.htm, Erişim Tarihi:23.05.2016
[29] *İnternet:* http://www.milliyet.com.tr/dolandiricilar-15-gunlugune-oto-gundem-2190724/, Erişim Tarihi:23.05.2016
[30] *İnternet:* http://www.haberler.com/telefonla-dolandiricilara-milyonlarca-lira-8186554-haberi/, Erişim Tarihi:23.05.2016
[31] Ronald, C., Carver, C., Ferguson, A., "Phishing for user security awareness", Computers & Security 26(1): pp. 73-80, 2007
[32] *İnternet:* http://www.bursa.pol.tr/Duyurular/Sayfalar/Kanma-Sen-Buna.aspx, Erişim Tarihi:24.05.2016
[33] *İnternet:* http://www.yeniakit.com.tr/haber/liseli-genc-dolandiricilari-dolandirdi-51969.html, Erişim Tarihi:24.05.2016
[34] *İnternet:* http://www.milliyet.com.tr/uyanik-vatandas-dolandiriciyi-gundem-2066228/, Erişim Tarihi:24.05.2016
[35] Kritzinger, E., and von Solms, S.H. 2010. "Cyber Security for Home Users: A New Way of Protection through Awareness Enforcement," Computers & Security 29:8, pp. 840- 847.