SOSYAL MÜHENDİSLİK VE DENETİM

Hasan BAĞCI
İç Denetçi
Dışişleri Bakanlığı

ÖZET: *Bilgisayar sistemleri insandan bağımsız olmadığı gibi, insan unsuru da güvenlik sisteminin en zayıf halkasıdır. Sosyal mühendisler, güvenlik zincirinin en zayıf halkasını oluşturan insan unsuruna odaklanıp kurumların savunma mekanizmalarını etkisiz hale getirmeye çalışmakta ve her türlü güvenlik açığını menfaatleri doğrultusunda kullanmaktadırlar. İnsan unsurunun yer aldığı bir sistem içinde sosyal mühendislik saldırılarına karşı hiçbir bilgisayar güvenlik sisteminin kesin güvence sağladığı söylenemez. İnsan ilişkilerinin manipüle edilmesi yoluyla gerçekleştirilen sosyal mühendislik saldırılarındaki temel hedef, kurumsal bilgilerin ele geçirilmesi, ele geçirilen bilgilerin kurumlar aleyhine kullanılması, kurumsal bilgilere erişimin engellenmesi, kayıtlı bilgilerin silinmesi ve bilgilerin doğruluğunu etkileyecek değişiklikler yapılarak kurumların zarara uğratılması olabilmektedir. Kurumlar arası ortak veri tabanının veya ortak network (ağ) sisteminin kullanıldığı günümüzde, kurumlardaki güvenlik açıkları başka kurumların güvenlik açığı haline gelmekte, çoğu zaman kurumlar açısından kaybedilen itibar ve güvenin bedeli baştan alınacak tedbirlerin maliyetinden daha fazla olmaktadır. Sosyal mühendislik saldırı tipleri sürekli değişen ve kendini yenileyen bir yapıya sahip olduğu için, güvenlik önlemlerinin çoğu bu alanda gizlenmiş, kesin olarak tanımlanamayan ve savunmasız alanlara doğru yönelen sosyal mühendislik saldırılarına karşı kesin bir başarı sağlayamayacaktır. Sosyal mühendislik saldırılarına karşı, açıkları tam olarak kapatabilecek garanti edilmiş bir yöntem bulunmamakla birlikte, eğitim-öğretim programları ve denetimler sayesinde riskleri hafifletebilecek ve zararları minimize edebilecek yöntemler bulmak mümkündür. Sosyal mühendisliğe karşı geliştirilen savunma mekanizmalarının düzenli olarak gözden geçirilmesi ve güncellenmesi, düzenli denetimler sayesinde zayıflıklarının tespit edilip etkinliklerinin onaylanması ve daha iyi politikaların geliştirilmesi önem kazanmaktadır.*

ANAHTAR SÖZCÜKLER: *Sosyal mühendislik, bilgi güvenliği, bilgi sistemleri, bilgi sistemleri denetimi, network sistemleri.*

GİRİŞ

Ekonomik veya stratejik değer ifade eden her türlü bilginin saldırı hedefi haline geldiği günümüzde bilginin kullanımı yetmemekte, bilginin korunması ve sağlıklı şekilde iletilmesi de önem kazanmaktadır. Çoğu kurumlar hacker'lere (sistem kırıcılara), karşı savunmaya geçmekte, firewall (güvenlik duvarları) politikasına odaklanmakta, internetten gelecek tehditlere karşı server'larını güçlendirmekte, kurum içi dosya transferlerinde network güvenliğini sağlamaya yönelik tedbirleri artırmaktadırlar.

Dünyada hiçbir bilgisayar sistemi insandan bağımsız değildir. İnsan unsuru aynı zamanda güvenlik sisteminin en zayıf halkasıdır. Hacker'ler güvenliğin insan boyutunu manipüle ederek sosyal mühendisliğe yönelmekte, her türlü güvenlik açığını menfaatleri doğrultusunda kullanmaktadırlar. Gerçekte çoğu kuruluş bilgi güvenliği açıklarını olayların meydana geldiği ana kadar görememekte, hatta ortak veri tabanının veya ortak ağ sisteminin kullanıldığı durumlarda sosyal mühendislik olaylarının hangi kurumların zafiyetlerinden kaynaklandığının anlaşılması da imkânsız hale gelmektedir.

Sosyal mühendislik olaylarına karşı yeterli bir korunma sağlayabilmek için belirlenecek politika ve prosedürler neler olmalıdır? Uygulamada etkili bir güvenlik sistemi nasıl sağlanmalıdır? Bu soruların cevabı, düzenli bir denetim sayesinde güvenlik politikasındaki eksikliklerin tespit edilip giderilmesiyle sağlanabilir. Ancak yapılacak denetimlerin çoğu bu alanda gizlenmiş, kesin olarak tanımlanamayan, savunmasız alanlara doğru yönelen sosyal mühendislik saldırılarına karşı kesin başarı sağlayamayacaktır.

Sosyal Mühendislik Nedir?

Sosyal mühendislik; etkileme, zorlama, aldatıcı ilişkiler geliştirme, sorumluluğu, etik değerleri, dürüstlüğü ya da bağlılığı azaltma amacını güden yöntemler kullanarak kişileri gizli bilgi vermeleri veya erişim sağlamaları için aldatma sürecidir. Ayrıca sosyal mühendislik; "organizasyon güvenliğinin insanlarla etkileşime girilerek kırılmasıdır" şeklinde tanımlandığı gibi, "insanların ortak duygularındaki boşluklardan avantajlar elde etmek" şeklinde de tanımlanmaktadır.

"Sosyal mühendislik; etkileme, zorlama, aldatıcı ilişkiler geliştirme, sorumluluğu, etik değerleri, dürüstlüğü ya da bağlılığı azaltma amacını güden yöntemler kullanarak kişileri gizli bilgi vermeleri veya erişim sağlamaları için aldatma sürecidir.**"**

Karakteristik olarak hacking "teknik vasıtalarla yasaklanmış sistemlere girmeye çalışmayı" ifade eder. Hacking olayında hacker "güvenlik boşluklarından avantajlar elde etmeye çalışırken", sosyal mühendis normal yollardan elde edemeyeceği bilgileri (örneğin şifreler, kripto anahtarları, kullanıcı ID'leri gibi) personeli manipüle ederek elde etmeye çalışır.[1] Sonuçta, sosyal mühendislik teknik vasıtalar kullanarak ele geçirilmesi son derece zor olan bilgileri elde etmek için kullanılan bir yöntemdir. Sosyal mühendislik tekniklerinin çoğu insanlardaki psikolojik özelliklerin istismar edilmesine dayanmaktadır.[2] Özetle sosyal mühendislik, iletişim (kişiler arası, kişiyle kurum arası, kurumlar arası) açıklıklarından ya da insan davranışlarındaki istismara açık alanlardan faydalanarak güvenlik süreçlerini etkisiz hale getirme yöntemlerine dayanan yasadışı müdahale süreçleridir.

Sosyal Mühendislik Saldırılarıyla Elde Edilmek İstenen Nedir?

Değer ifade eden her türlü bilginin saldırı hedefi haline geldiği günümüzde, çoğu kişi veya kurum sosyal mühendislik saldırılarına hedef olmakta, saldırı sonucunda çeşitli risklerle karşı karşıya kalmaktadır. Çoğu zaman yanlışlıkla söylenen bir kullanıcı şifresinin ku-

1 Social Engineering: Understanding and Auditing-GSEC Practical Assignment- By Chris Jones–4/11/2003 http://www.sans.org/reading_room/whitepapers/engineering/understanding_and_auditing_1332

2 Social Engineering - The Weakest Link in Information Security - Jeff Mc Dermott http://www.windowsecurity.com/whitepapers/Social-Engineering-The-Weakest-Link.html

ruma ait en hassas bilgilerin dışarıya sızmasına neden olduğu görülmektedir.

Sosyal mühendislik saldırılarında amaç hedeflenen sistem yada network yapısını bozup kullanılamaz duruma getirmek olabileceği gibi, kurumsal network yapısı, işletim sistemi versiyonu, kimlik hırsızlığı, kripto anahtarları, yazılım versiyonları, çalışanların ve yöneticilerin kişisel bilgileri, şifreler ve saldırıda kullanılabilecek her türlü materyalin toplanması olabilmektedir.

Saldırganlar ele geçirdikleri şifrelerle erişimi kısıtlı dosyaları indirmekte veya bant genişliği, işlemci zamanı, disk alanı gibi sınırlı kaynakları kullanarak hizmet hırsızlığı yapmaktadırlar. Kurumlara ait bilgileri ele geçiren saldırganlar, bu bilgileri ya daha fazla suiistimal için kullanmakta, ya da kurum aleyhine olacak şekilde (bilgilerin satılması v.b.) değerlendirmektedirler. Bunun yanında saldırganlar kurumlara zarar vermek istediklerinde, kurum bilgilerini erişimi engelleyebilmekte, kayıtlı bilgileri silmekte veya bilgilerin doğruluğunu etkileyecek şekilde değişiklikler yaparak kurumları zarara uğratmaktadırlar.

Kimi sosyal mühendislik saldırılarında asıl amaç kurumsal güvenin sarsılması ve kurumların itibar kaybına uğratılması olabilmektedir. Sosyal mühendislik yoluyla zarara uğramış kurumlar İtibar ve güven kaybına uğramaktalar, kaybedilen İtibar ve güvenin bedeli baştan alınacak tedbirlerin maliyetinden daha fazla olmaktadır.

Ortak veri tabanının veya ortak network sisteminin kullanıldığı durumlarda, kurumlardaki güvenlik açıkları başka kurumların güvenlik açığı haline gelmektedir. Böyle durumlarda hangi kurumdaki zafiyetin sosyal mühendislik saldırılarına davetiye çıkardığı da anlaşılmaz hale gelmektedir. Ayrıca sosyal mühendislik saldırılarıyla ele geçirilen sistem ve kaynaklar, başka sistem ve kaynakların ele geçirilmesi veya zarar verilmesi için kullanılabilmektedir. Dolaylı olarak kurumların güvenlik açıkları başka kurumlara yapılacak saldırılara sebep olmaktadır.

Sosyal Mühendislik Saldırılarının Hedefleri Kimlerdir?

Kurumlara yönelik sosyal mühendislik saldırılarında, saldırganın suiistimal edebileceği durumdaki personelin tamamı hedef olabilmektedir. Sosyal mühendislik saldırılarında hedef seçilen kişiler:

a) **Doğrudan ulaşılabilir personel**: Kurumların dışa bakan yönü olarak tanımlanan, yaptıkları iş gereği dışarıdan gelen kişilerle doğrudan iletişime geçen personel (müracaat görevlileri, güvenlik görevlileri, telefon santrali görevlileri v.b.). [3]
b) **Üst düzey yöneticiler ve önemli personel:** Kurumdaki görevleri gereği zorunlu olarak ayrıcalıklı yetkiye sahip olan veya gizli bilgiye çeşitli nedenlerle erişim hakkı olan çalışanlar. Kendilerine sistem üzerinde sınırsız erişim yetkisi sağlayan şifreler verilen, ancak eksik bilgilendirme veya mesailerinin yoğunluğu nedeniyle kendilerine verilen şifreleri hatırlamakta bile zorlanan, bu nedenle çok basit şifreler kullanan, hatta şifrelerini bir yerlere yazarak hatırlamaya çalışan ya da yanında çalıştırdığı kişilere (sekreter, hizmetli, v.b.) şifrelerini emanet eden yöneticiler sosyal mühendislik saldırılarının hedefi olabilmektedir.
c) **Zaafları olan, aldatılmaya, ikna edilmeye uygun personel:** Kuruma ya da kurum çalışanlarına bağlılığı zayıflamış, zaafları olan, aldatılmaya, ikna edilmeye müsait olan her düzeydeki personel.
d) **Faydalı olmaya istekli sempatik personel:** Diğer insanlara yardım etmekten zevk alan görev ve yetkisini aşarak yardım ve destek talebinde bulunanların imdadına koşan, sempatik tavırlar sergileyerek yetki ve itibar elde etmeye çalışan personel. Saldırganlar bu tür çalışanlardan giriş hakkı isteyerek veya bir hesaba giriş için yardım etmesini dileyerek işe başlarlar, ayrıca birçok bireyin zayıf reddetme düzeyini bildiklerinden işin uzmanına danışıyormuş havasını vererek bu kişilerden hassas bilgileri elde etmeye çalışırlar.[4]
e) **Desteğe muhtaç personel veya kullanıcılar:** Kurum hizmetlerinden yararlandıkları için sistemlere erişim hakkı verilen ancak sistem hakkında yeterli bilgisi olmayan, bu nedenle yardıma ihtiyaç duyduklarında kurumsal destek veren personelle saldırganı ayırt edemeyecek durumdaki personel veya kullanıcılar.[5]
f) **Bağlılık seviyesi düşük personel:** Kurumun hedef

3 Can Bican - Sosyal Mühendislik Saldırıları - http://www.bican.net/2008/05/20/sosyal-muhendislik-saldirilari/
4 Can Bican – a.g.e.
5 Can Bican – a.g.e.

ve politikalarını kavraması zor olan, bilhassa alt kademelerde çalışan personel (sıradan memurlar, güvenlik görevlileri, resepsiyon görevlileri, hizmetliler v.b). Saldırganın sorduğu sorularla neyi elde etmeye çalıştığını anlayabilecek kabiliyeti olmayan, yaptıkları görevin gerekleriyle kendilerine yöneltilen sorular arasındaki ilişkiyi tam olarak kavrayamayan çalışanlar en kolay saldırı hedefidirler.

Sosyal Mühendislik Teknikleri Nelerdir?

Sosyal mühendisler insanları sorularla veya farklı yöntemlerle kandırmak suretiyle kurumlara veya kişilere ait bilgileri fark ettirmeden almaya çalıştıkları için değişik saldırı teknikleri uygulamaktadırlar.[6] Kurumlara çalışan olarak sızmak, çalışanlarla arkadaş olmak, teknik servis ya da destek alınan bir kurumdan arıyormuş gibi görünerek bilgi toplamak, hedef kişiyle dost olunarak kişilerin zaaf ve düşkünlüklerinden yararlanmak, hedef seçilen kişilerin şifrelerini elde etmek için elektronik postalarına (e-maillerine) tuzak mesajlar atmak, sistem sorumlusu olduğunu söyleyerek kullanıcıların şifrelerini öğrenmeye çalışmak, teknisyen kılığında kurum içerisine fiziksel olarak sızmak veya çöpleri karıştırarak bilgi toplamak en fazla bilinen sosyal mühendislik yöntemleridir.[7]

Sosyal mühendislik saldırılarında saldırının nereden geleceğini bilebilmek faydalı olabileceği gibi, saldırının ne şekilde olacağını anlamak da önemlidir. Sosyal mühendisler kurbanlarına karşı çok çeşitli psikolojik saldırı yöntemleri kullanmaktadırlar. Bu yöntemlerden bazıları şöyledir:

a) Otorite: İnsanları aldatmak için üst düzey yetkili biri olduğunu veya itibarlı bir müşteri olduğunu ikna etmek en fazla kullanılan yöntemlerden biridir.[8]

b) Bağlantı ve Benzerlik: Hedef seçilen kişilerle yakın temasa geçilip, kişisel bağlantılar kurularak, ipuçları yakalanmaya çalışılmasıdır. İnsanlar kendilerine benzeyen kişilere yakınlık duyduğu için sosyal mühendisler bu durumu ihmal etmeyecektir. Öncelikle hedefteki kişinin bireysel ilgi alanlarına yönelik (kişilerin siyasi eğilimleri, hobileri, sevdiği filimler, tuttuğu takımlar v.b.) bağlantılar kurularak, muhataba güven duygusu verilip ikna yollu ataklar gerçekleştirilmesidir.

c) Mukabele etmek: Yapılan bir iyilik için bir karşılık önermek. Çoğunlukla belirlenen kurbanlar ile güvenilir bir ilişki ortamı geliştirilip, küçük etkileşimlerle ilişkiye girilerek güven ilişkisinin sömürüleceği zamanın beklenmesidir.

d) **Birbirine göre ayarlama:** Hedef ile çatışmaya girmeme en iyi durum olduğu için ortamın gerektirdiği ses tonu ile zekice ve sabırlı bir sunuş yapılmasıdır. Sinirli hareketler, emir cümlelerinin kullanılması veya bir şey sipariş eder gibi talimat verilme si en son tercih edilecek yöntemlerdir. Bu nedenle rica etme, uydurma durum belirleme, kişisel ikna gibi metotlar daha fazla kullanılmaktadır.[9]

e) **Uydurma durum:** Bir olay veya bir organizasyonun özelliğine göre elde edilen bilgilerle üretilen suni bir durum, bir kriz veya özel bir an ile ilgili olarak bu durumdan faydalanmadır.[10] Sosyal mühendisler anlık yardım içeren kriz durumlarını çok iyi kullanabildikleri gibi, çalışanların güvenlerini sarsmadan yardım edilme ile ilgili suni ortamları oluşturmaya yönelik taktikler kullanmaktadırlar.

f) Doğal eğilimlerin kullanılması: İnsanların en doğal özelliği olan, başkalarına yardım etme duygu ve eğilimlerinin kullanılmasıdır. Yardıma muhtaç müşteri gibi davranma ya da çalışanları yetkili personel olduğuna inandırarak onların açıklıklarından faydalanmak en fazla kullanılan yöntemlerdendir.[11]

g) **Sorumluluğun yayılımı**: Çalışanların sadece kendi hareketlerinden sorumlu olmadıkları, başkalarının görev alanına giren konulardan da sorumlu olduklarına inandırılması yöntemidir. Sosyal mühendisler çeşitli faktörlerin de yardımı ile oluşturdukları ortamlarda, kişisel sorumluluk konusunu abartarak çalışanları şaşırtırlar ve bir karar vermeye

6 A Proactive Defence to Social Engineering - http://www.sans.org/reading_room/whitepapers/engineering/511.php

7 "Social Engineering"-http://www.hq.nasa.gov/office/ospp/securityguide/V1comput/Social.htm

8 The Threat of Social Engineering and Your Defense Against It http://www.sans.org/reading_room/whitepapers/engineering/the_threat_of_social_engineering_and_your_defense_against_it_1232?show=1232.php&cat=engineering

9 Güven Şeker - İnternette Bilişim Suçlarında Kullanılan Metotlar-http://uretim.meb.gov.tr/EgitekHaber/s75/b%C4%B1ls%C4%B1m%20suclar%C4%B1.htm

10 Güven Şeker – a.g.e

11 Social Engineering: Understanding and Auditing - GSEC Practical Assignment - a.g.e

zorlarlar. Karar verme sürecinde diğer çalışanların isimlerinin kullanılması veya yüksek mevkiden yetkilendirilmiş bir görev olduğunun iddia edilmesi bilinen yöntemlerdendir.[12]

h) **Bağlılık ve dürüstlüğün suiistimali:** Öncelikle hedef seçilen kişin zaafları tespit edilerek, zaafların kurum ve kişi aleyhine olacak şekilde kullanılması, kurum çıkarlarıyla bağdaşmayacak hareketlerin yapılması sağlanarak kurumsal bağlılığın zayıflatılmasıdır. Kurumsal bağlılığı zayıflamış, dürüstlük kurallarını ihmal etmiş çalışanlar kullanılmaya hazır hale gelmiştir.[13]

Sosyal Mühendislik Saldırılarına Karşı Savunma Yöntemleri

Sosyal mühendislik saldırılarına karşı, açıkları tam olarak kapatabilecek garanti edilmiş bir yöntem bulunmamakla birlikte, riskleri hafifletebilecek ve zararları minimize edebilecek yöntemler bulmak mümkündür. Siber saldırılara karşı bilgisayar ve network altyapısına yönelik tedbirler alınırken sosyal mühendislik saldırılarına karşı daha farklı savunma yöntemlerinin geliştirilmesi gerekmektedir. Bilinen teknik hackerlik saldırılarından farklı olarak sosyal mühendislik saldırılarında çalışan kişilerin bilgi düzeyleri ve kimlikleri önem kazanmaktadır. Özellikle bilgilerin yüksek hassaslık derecesine sahip olduğu hissedilen yerlerde, saldırılar yüksek seviyede teknik bilgiye sahip kişileri hedef alabileceği gibi, büro temizlik görevlisi veya gece bekçisi gibi düşük seviyede bilgiye sahip bireyleri de hedef alabilmektedir.[14]

Sosyal mühendisler, güvenlik zincirinin en zayıf halkasını oluşturan insan unsuruna odaklanıp kurumların savunma mekanizmalarını etkisiz hale getirmeye çalışmaktadırlar. İnsan unsurunun yer aldığı bir sistem içinde sosyal mühendislik saldırılarına karşı hiçbir bilgisayar güvenlik sisteminin kesin güvence sağladığı söylenemez. Bundan dolayı insan faktörünün istismarına dayanan sosyal mühendislik saldırılarının her an olabileceği unutulmamalıdır.

Saldırılara Karşı En Etkili Savunma Yöntemi: Eğitim ve Öğretim

Başarılı bir güvenlik düzenlemesi yapabilmek için, yapılan işin her aşamasında ve bölümünde çalışanların kullandıkları bilgisayarlara ilişkin güvenlik düzenlemelerinin yapılması zorunludur. Organizasyonda yer alan kişilere güvenliğe ilişkin bilgilerin tam olarak anlatılması, çalışanlara network güvenliğine ilişkin sorumluluk duygusunun verilmesi organizasyon yararına olacaktır. Gerçekte, en etkili savunma kişilerin sosyal mühendislik saldırılarıyla her an istismar edilebileceğinin öğretilmesidir.[15]

Kurum çalışanlarının kimliğini kanıtlamayan kişilere kesinlikle bilgi aktarmaması, iş hayatı ile özel hayatlarını birbirinden ayırmaları hususunda gerekli uyarılar yapılmalı ve önlemler alınmalıdır. Bu nedenle çalışanlara güvenlik öngörüleri ve güvenlik bilgileri alanında bilgi güvenliği farkındalığı programı uygulanmalıdır.[16] Çalışanların sosyal mühendislik saldırılarına karşı eğitilmeleri kurumlar açısından en etkili savunma aracı olacaktır. Esasen sosyal mühendislik saldırılarına karşı en etkili savunma yönteminin eğitim ve öğretim olduğu unutulmamalıdır.

Eğitim ve Öğretimin Haricinde Kullanılabilecek Diğer Tedbirler

a) Fiziki Güvenliğin Geliştirilmesi: Öncelikle kurumlardaki hassas içerikli bilgilerin saldırılara karşı fiziki güvenliğinin sağlanması gerekmektedir. Fiziki güvenliğin geliştirilmesi dışarıdaki saldırganlara karşı faydalı olabilecektir, ancak saldırganın içeriden biri olması durumunda etkin bir fiziki savunmadan bahsedilemeyecektir. Bu nedenle sistemlere fiziksel erişim imkânı olan kişilerin güvenilir olup olmadığı gözden geçirilmeli, fiziksel tehditlerin olma olasılığına göre gerekli tedbirler alınmalıdır. Bunun yanında kurumlardaki çeşitli kullanıcı profillerinin sisteme erişim imkânları göz önüne alınarak, kullanıcı güvenlik politikalarındaki sıkılaştırmalara önem verilmeli, tüm kullanıcı profillerinin yetkileri belirlenmelidir.

12 Güven Şeker – a.g.e

13 Social Engineering: Understanding and Auditing - GSEC Practical Assignment - a.g.e.

14 Social engineering attacks: What we can learn from Kevin Mitnick - Mark T. Edmead http://searchfinancialsecurity.techtarget.com/tip/0,289483,sid185_gci1294530,00.html

15 The Threat of Social Engineering and Your Defense Against It – a.g.e.

16 Fighting Social Engineering - Mikael Hermansson & Robert Ravne - University of Stockholm / Royal Institute of Technology - March 2005 - http://dsv.su.se/en/seclab/pages/pdf-files/2005-x-281.pdf

b) Güçlü Güvenlik Politikası: Hassas bilgilere yönelik güçlü kontrol sistemlerinin oluşturulması sosyal mühendisler için caydırıcı bir unsurdur. Kurumun oluşturduğu güvenlik politikaları açık, anlaşılır, makul, uygulanabilir, erişilebilir ve kapsayıcı olmalıdır. Kontrol sistemleri eğitim ve öğretimle desteklenerek güçlendirilmelidir. Çalışanlara kurumun güvenlik politikaları hakkında eğitimler verilerek, güvenlikle ilgili görev ve sorumluklar öğretilmelidir. Güvenlik politikaları hazırlanırken kurumla çalışanlar arasında makul bir güven seviyesi belirlenmelidir. [17] Çalışanlara yeterince güvenilmemesi durumunda çalışanların kuruma bağlılığı zayıflayacak, gereğinden fazla güven duyulması durumunda ise çalışanlardan ya da çalışanlar üzerinden gelecek saldırılara karşı sistem savunmasız bırakılmış olacaktır.

c) Şifre Güvenliği Politikası: Sistemlerde yer alan her türlü bilginin şifrelerle korunduğu, bu bilgilere ancak şifreler yardımıyla ulaşılabilindiği bir ortamda, saldırganlar için en önemli hedef kullanıcı şifreleri olmaktadır. Şifreler kullanıcıların ulaşmak istedikleri bilgilere erişim yetkilerinin olup olmadığının denetlenmesine yarayan bir araç olduğundan, şifrelerin yanlış ve kötü amaçlı kullanımları güvenlik sorunlarına yol açabilecektir.

Kullanıcı hesaplarının izinsiz kullanımına karşı, kullanıcıların basit ve kolay tahmin edilebilir şifreler seçmeleri engellenmeli, kriterlere uymayan zayıf şifreler saptanıp gereken uyarılar yapılmalı, gerektiğinde şifre seçimlerine müdahale edilmeli, bu konuda çalışanlar bilinçlendirilmelidir. Kullanıcı şifrelerinin tahmin edilebilecek kadar kolay olduğu, hatta bazı kimselerin iş bilgisayarlarına şifre atamadığı ya da şifrelerini bir kâğıda yazıp masa üstüne bıraktığı söz konusu olabilmektedir. Saldırganlar kullanıcı şifrelerini tahmin edebilmek için muhtemel şifreleri deneyerek doğru şifreyi bulmaya çalışırlar, hatta otomatikleştirilmiş programlar sayesinde çok sayıda şifreyi kısa sürede deneyebilirler. Bu nedenle üst üste belirli bir sınırın üzerinde yanlış şifre girildiğinde kullanıcı hesabını devre dışı bırakacak güvenlik mekanizmaları kullanılmalıdır. Her hesap için ayrı bir şifre kullanılmalı ve şifreler belli aralıklarla değiştirilmeli, ayrıca kullanıcılar şifrelerinin çalındığından veya kullanıcı hesaplarına izinsiz girildiğinden kuşkulandıkları durumlarda uygulanması geren prosedürler belirlenerek gereken önlemler alınmalıdır. [18]

d) Güvenlik Kurallarına Uymamanın Müeyyidesi: Uygulanmakta olan kurumsal güvenlik politikalarına verilen önem çalışanlar tarafından yeterince anlaşılamadıysa güvenlik politikalarının fazlaca bir değeri olmayacaktır. Eğim ve öğretimle beraber güvenlik kontrollerinin düzenli bir şekilde yapılması, çalışanların uygulanmakta olan politikaların önemi hakkında farkındalıklarının sağlanması gerekmektedir.[19] Ayrıca yapılan kontrollerde güvenlik politikalarına aykırı davranışlarda bulunanların üst yönetim tarafından cezalandırılacağı ve güvenlik ihlallerinin affedilmeyeceği bilincinin yerleştirilmesi gerekmektedir. Eğitime ek olarak uygulanan yaptırımlar çalışanların güvenlik politikalarını izlemesine yardımcı olacaktır.

e) Yönetim Prosedürlerindeki Olayların Detaylandırılması: Saldırılara karşı bilinçlendirme faaliyetleri önemli olduğu kadar, saldırı anında uygulanacak yöntemlerin ve yapılacak işlerin belirlenmesi de önemlidir.[20] Kurum çalışanlarıyla irtibata geçmeye çalışan kişilerin kimliklerinin nasıl doğrulanacağı, saldırı olayını fark eden personelin ilk önce hangi yetkiliye müracaat edeceği, kullanıcıların elektronik posta iletilerinin asıl kaynaklarını nasıl belirleyecekleri, şüpheli elektronik postaları nasıl işleyecekleri, web adreslerinin kimlik doğrulama bilgilerini nasıl kontrol edecekleri gibi detaylandırılmış prosedürlerin hazırlanıp uygulamaya geçirilmesi gerekmektedir. Sosyal mühendislik saldırıları çoğunlukla kişisel zaaflar kullanılarak yapıldığından, hedef seçilen kişiler saldırının farkına varmayabilir ya da fark etse bile kendi itibar ve güvenilirliğini zedeleyeceğini düşündüğü için olayı ilgili makamlara iletmeyebilir. Bu yüzden saldırı meydana geldikten sonra durumun yetkili personele iletilmesi için gerekli prosedürler oluşturulmalıdır.

17 Bilgisayar Ağlarında Güvenlik Politikalarının Uygulaması - Ar. Gör. Enis Karaarslan, Abdullah Teke, Prof. Dr. Halil Şengonca http://csirt.ulakbim.gov.tr/dokumanlar/BilgisayarAglarindaGuvenlikPolitikalarininUygulanmasi.pdf

18 Bilgisayar Ağlarında Güvenlik Politikalarının Uygulaması – a.g.e

19 A Proactive Defence to Social Engineering http://www.sans.org/reading_room/whitepapers/engineering/511.php

20 The Threat of Social Engineering and Your Defense Against It- a.g.e

Denetim

Sosyal mühendislik saldırına ilişkin plan ve taktikler incelendiğinde, sosyal mühendisliğin güvenlik sisteminin parçası olan insana karşı yapıldığı görülmektedir. İnsanların zekâ gücü ve geçmişte yaşadıkları tecrübeler birbirlerinden farklı olduğu için insan davranışlarının önceden tahmin edilmesi imkânsızdır. Bu nedenle güvenlik önlemlerinin çoğu bu alanda gizlenmiş, kesin olarak tanımlanamayan, savunmasız alanlara doğru yönelen sosyal mühendislik saldırılarına karşı kesin bir başarı sağlayamayacaktır.

Çoğu kurum sosyal mühendislikle mücadele için eğitimler düzenlemekte, yeni politika ve prosedürler hazırlamakta, ancak bunların etki ve güvenilirliğini sosyal mühendislik saldırıları meydana geldiğinde görebilmektedir. Sosyal mühendislik saldırı tipleri sürekli değişen ve kendini yenileyen bir yapıya sahip olduğu için, saldırılara karşı alınan önlemlerin ve oluşturulan güvenlik politikalarının düzenli olarak gözden geçirilmesi ve güncellenmesi, denetimlerle etkinliklerinin onaylanması gereklidir.

Güvenlik politikası eğitim ve öğretimiyle, çalışanlara ne şekilde hareket edecekleri, nasıl davranacakları hususunda daha iyi rehberlik edebiliriz. Ancak ciddiyetsizlik ya da bilgisizliğin olduğu durumlarda güçlü bilgi kontrolünün sağlanması nasıl olacak? Alınan tedbirlerin kurumu korumaya yeterli olup olmadığını nasıl bileceğiz? Buna benzer pek çok soru sosyal mühendislik denetimlerini zorunlu kılmaktadır.

Sosyal mühendisliğe karşı geliştirilen savunma mekanizmaları genelde güvenlik politikalarının güçlendirilmesi, düzenli denetimler sayesinde zayıflıkların tespit edilmesi ve daha iyi politikalarının geliştirilmesidir. Sosyal mühendislik denetimleri kurumların güvenlik farkındalığı programlarında önemli bir yer tutmaktadır. Çalışanların, yaptıkları işin bir parçası olarak güvenlik politikalarından haberdar olmaları ve politika kurallarına uymaları yapılan kontrolleri daha etkin kılacaktır. Sosyal mühendislik denetimleri sayesinde sosyal mühendislik saldırılarına karşı odaklanmış kurumlarda, çalışanların bu tür saldırılara daha az hedef oldukları tespit edilmiştir.

Sosyal Mühendislik Denetim Teknikleri

Denetimin planlanması, sosyal mühendisliğin tam olarak anlaşılması ve buna karşı alınacak önlemlerin belirlenmesi neticesinde mümkün olacaktır. Sosyal mühendislik saldırıları; bilgi toplama, ilişki kurma, istismar ve erişim olmak üzere dört aşamada gerçekleşmektedir.[21] Uygulanacak denetim süreci bir saldırganın yapması beklenenlerin tatbikatı şeklinde olacağından, denetimin planlanması ve denetim süreci de saldırı aşamalarının sırayla denenmesi şeklinde olacaktır.

"Sosyal mühendisliğe karşı geliştirilen savunma mekanizmaları genelde güvenlik politikalarının güçlendirilmesi, düzenli denetimler sayesinde zayıflıkların tespit edilmesi ve daha iyi politikalarının geliştirilmesidir. Sosyal mühendislik denetimleri kurumların güvenlik farkındalığı programlarında önemli bir yer tutmaktadır."

Sosyal mühendislik olaylarına karşı gerçekleştirilecek denetimler aşağıdaki süreçlerden meydana gelmektedir.

a) Denetime hazırlık aşaması

Denetime başlamadan evvel, kurumların önceden belirlenmiş denetim programı ve uygulaması yoksa belirli bir zaman diliminin hazırlık aşamasına ayrılması gerekmektedir. Denetimlerin amacı organizasyonda yer alan birimlerin hesap verebilirliğinin sağlanmasına yönelik olduğu için, öncelikle organizasyonda yer alan birimlerin görev tanımlarının yapılmış olması gerekecektir. Denetim programı hazırlanırken kontrol sistemlerinin yerleşmesine yönelik aktivitelerin incelenmesi, yeni politikalarla belirlenen güvenlik sistemlerinin test edilmesin sağlanması, yasadışı aktivitelerin ortaya çıkarılması gibi hususlar dikkate alınmalıdır.

Denetim teknikleri ve denetim süreci bir saldırgandan beklenen hareketlerin tatbikatı şeklinde olacağından çalışanlar tarafından yetkisiz aktivite olarak değerlendirilebilecektir. Bu nedenle denetime başlamadan

21 Social Engineering: Understanding and Auditing - GSEC Practical Assignment - a.g.e.

önce üst yöneticiden yetki alınması, yetki almaksızın herhangi bir güvenlik testi uygulamasına geçilmemesi gerekmektedir. Ayrıca denetime başlamadan önce, denetimler kurum çalışanlarına uygun bir şekilde bildirilmelidir.[22]

Denetime hazırlık aşamasında, objektif bir denetim planının oluşturulması için güncel politika ve mevzuatın araştırılması zorunludur. Güncel politika ve mevzuatın araştırılması, denetimlerde farklı seviyelerdeki çıktıların bölümlenerek, hangi tür kontrollerin gerçekleştirilmesi gerektiği hususunda bizlere yardımcı olacaktır.

b) İstihbarat toplama aşaması

Sosyal mühendisler bilgisiz veya eksik bilgi sahibi kişilerin yetersizliklerini kullanarak saldırıya başlarlar. Bundan dolayı saldırı öncesinde geniş bir bilgi toplama kampanyası yürütürler. Şirket hakkında bilgi toplanması, bilgilerin denenmesi, şirket kültürü ve çalışanların tanınması, hedefteki potansiyel zayıflıkların tespiti başlangıç aşamasında önem taşır. Sosyal mühendisler için çalışanların listesi, dâhili telefon numaraları, kurumsal elektronik posta adresleri, ortak yönlendirici yetkileri ve hassas güvenlik bilgileri hayati önem taşımaktadır.

İstihbarat toplama aşamasında çoğu zaman kurumsal web sayfalarından, arama motorlarından, haber gruplarından, forumlardan ve iş arama sitelerinden kurum çalışanları ve kurum organizasyonu hakkında yeterli bilgi edinilebilmektedir. Denetimlerde bu ortamlardan kuruma ait hassas bilgilerin ne kadarının elde edilebileceği üzerine yoğunlaşılmalıdır.

Kurumsal web-siteleri – İşe ilk başlanacak yer kurumun web-sitesidir. Şirket yöneticileri, çalışanlar ve şirket hakkında yayınlanan broşürler sosyal mühendisler için zengin bir bilgi kaynağı olabilmektedir. Bu nedenle ortak kullanım amacıyla web-sitelerine veya broşürlere konulmuş her türlü kurumsal veya kişisel bilginin kurumlar için potansiyel problem kaynağı olabileceği düşünülerek, bu tür bilgilerin içeriğinin gözden geçirilmesi faydalı olacaktır.

Arama motorları – Arama motorlarından kurumlar hakkında pek çok bilgi elde edebiliriz. Kurum çalışanlarıyla ilgili bilgiler, kurumun ilişki içinde olduğu veya birlikte çalıştığı kurumlar/kişiler, hatta kurum müşterilerinin kimler olduğu gibi genel bilgileri arama motorlarından bulabiliriz. Kurumun çok büyük ve iyi bilinen bir kurum olması durumunda arama motorlarından daha çok bilgi elde edilebilecektir. Kurum hakkında haber sitelerinde yer alan bilgilerin gerçekliğinin doğrulanması, kuruma ait ve kurum güvenliğini tehdit eden hassas bilgilerin dışarıya sızıp sızmadığının araştırılması faydalı olacaktır.[23] Ayrıca kurum çalışanlarının forum sitelerinde kuruma ait bilgileri paylaştığı durumlar da olabilmektedir. Çalışanların kuruma ait hangi tip bilgileri web ortamında paylaştığı hususunda genel bir bilgi edinilmelidir.

Haber grupları – Sosyal mühendisler kurumsal bilgileri ele geçirebilmek için haber gruplarından faydalanırlar. Arama motorlarında yer alan haber gruplarındaki bilgiler araştırma yapmak için mükemmel bir kaynak oluşturmaktadır.[24] Ayrıca kurumla ilgili olarak kurum çalışanları tarafından yazılan makaleleri de haber gruplarında bulmak mümkündür. Haber gruplarında bazı kurum çalışanlarının, hatta sistem yöneticisi konumundaki uzmanların sistemdeki güvenlik duvarları ile ilgili bilgileri tanımadıkları kişilerle rahatça paylaştıkları görülmüştür. Bu nedenle denetime hazırlık aşamasında haber gruplarında gezinti yapıp kurumla ilgili bilgileri derlemeye çalışmak faydalı olabilecektir.
İş arama siteleri – İş arama sitelerinin araştırılması hassas bilgilerin ortaya çıkarılmasında pek fazla işe yaramayacaktır. Ancak İş arama siteleri bir kurumun personel açısından yapısının ne olduğu ve personel açığının hangi alanlarda olduğu hususunda mükemmel bir bilgi kaynağıdır. Bu nedenle iş arama siteleri gözden geçirilerek, denetlenecek kurumla ilgili hangi tür bilgilerin yer aldığı, iş ilanlarında güvenlik kurallarına uyulup uyulmadığı hususları araştırılmalıdır.

c) Fiziksel giriş aşaması

Sosyal mühendisler başarı sağlayabilmek için şirket varlıkları üzerinde herhangi bir fiziki iz bırakmadan çalışmalarını sürdürürler, ancak bazı durumlarda daha ileri düzeyde bilgi elde edebilmek için kurum-

22 Social Engineering: Understanding and Auditing - GSEC Practical Assignment - a.g.e.

23 Social Engineering - The Weakest Link in Information Security - Jeff Mc Dermott- a.g.e

24 Social Engineering: Understanding and Auditing - GSEC Practical Assignment – a.g.e

lara fiziksel giriş yapmak isteyeceklerdir. Fiziksel giriş yapmak isteyen sosyal mühendisler güvenlik görevlilerini kandırmak, kurumların giriş kısımlarında bulunan kontrol noktalarından geçebilmek veya güvenliği sağlayan diğer vasıtaları atlatabilmek için değişik yöntemler deneyeceklerdir. Bunlar içinde en fazla kullanılan yöntem kurumda çalışan biri gibi davranarak (sahte kimlik kartı kullanma, çalışanların giydiği resmi kıyafetleri giyme, sahte rozetler takma v.b. şekilde) fiziksel giriş yapmayı denemektir. Bunun yanında işe giriş saatlerinde kalabalığa karışıp çalışanların arasından giriş yapmak, hizmet sağlayıcısı (postacı, tamirci v.b.) gibi davranmak, kurumla randevusu olan müşteri veya ziyaretçi gibi davranmak, kamu hizmeti veren başka kuruluş çalışanı gibi davranmak, normal süreçlerin uygulanmadığı mesai saatleri dışında giriş yapmaya çalışmak gibi yöntemler de bulunmaktadır.[25]

Denetimler sırasında sosyal mühendislerin kandırabileceği veya atlatabileceği güvenlik görevlilerinin, kontrol noktalarının ve güvenliği sağlayan diğer vasıtaların olup olmadığının gözden geçirilmesi, şüpheli durumlarda gereken tedbirlerin alınması sağlanmalıdır. Kurum çalışanları tarafından tanınan bir denetçinin bu tür aldatma yöntemini kullanarak sosyal mühendislik saldırıları yapılıp yapılmadığını anlamaya çalışması zor olacaktır. Bunun için çalışanların tanımadığı başka bir denetçi veya özel bir görevli tarafından çalışanların denenmesi, bu tür aldatma ve atlatma yöntemlerine açık olup olmadıklarının tespit edilmesi faydalı olacaktır.[26]

d) Fiziksel giriş sonrası

Fiziksel giriş aşamasından sonra sosyal mühendislerin önünde pek çok seçenek bulunmaktadır. Bu seçenekler arasında; kurum network'una korumasız giriş yapmak için açık bir network ucu elde etmeye çalışmak, hassas bilgileri çalmak için daha önceden hedef seçilen kişilerin bilgisayarındaki bilgilere ulaşmak, virüs yazılımları yüklemek, çalışanları gizlice izleyip (omuz sörfü, kulak misafirliği v.b. yollarla) şifrelerini ele geçirmek, ekranı kilitlenmemiş bilgisayarları kullanmak, kullanıcı bilgisayarlarını kullanıma açmaya ikna etmek, odalardaki korumasız evraklara göz atmak, çalışanların masalarında bulunan notları incelemek, kuruma ait çöpleri karıştırmak, takvimlere-ajandalara ve ortak kullanıma açık panolara göz atmak gibi seçenekler bulunmaktadır.[27]

Denetim sırasında, hassas bilgilerin yer aldığı dolap ve rafların yetkisiz erişimlere karşı kilitli olup olmadığı kontrol edilmelidir. Ayrıca uygulanan güvenlik politikalarıyla kurumsal bilgilerin gizlilik derecesine göre sınıflandırmaya tabi tutulup tutulmadığının, hassas bilgilerin çalışanlar tarafından güvenli olmayan alanlara çıkarılıp çıkarılmadığının kontrol edilmesi gerekmektedir.

e) Telefon bazlı denetim

Sosyal mühendisler için telefon önemli bir araçtır. Telefonlar saldırganların kendilerini belli etmeden çalışanlara yaklaşılmasını izin veren, çoğu zaman çalışanları savunmasız bırakan saldırı araçlarıdır.[28] Bu tür denetimlerde, denetim planı hazırlamak için düzenlenmiş birkaç temel nokta bulunmaktadır. Öncelikle sosyal mühendisin ele geçirmeyi amaçladığı bilgi tiplerinin neler olduğunun tanımlanması gerekmektedir. Bu bilgiler şifreler, hassas belgeler, ilave telefon numaraları veya saldırganın işine yarayacak diğer bilgiler olabilir. Öncelikle bilinmesi gerekir ki, saldırganlar elde etmek istedikleri bilgilerin tamamını karşılarına çıkan ilk kişiye sormak yerine, aşamalı olarak çalışanlar arasında bir güven zinciri oluşturmak suretiyle elde etmeyi tercih ederler.

Saldırıya ilk sırada hedef olan görevliler istenilen bilginin bakılmasını veya araştırılmasını kimin izin verdiğini sorabileceklerdir. Bu nedenle saldırgan hedef bir bilgiyi ele geçirmeyi amaçladığında, bilgiyi erişmede karşılaşılacağı ilk görevlileri tanımak isteyecektir. Saldırganın bilgilerin derlenmesinde kandırabileceği yani birlikte çalışabileceği görevlileri ve üst dereceli görevlileri tanıması gerektiğinden bu kişiler hakkında araştırma yapmak isteyecektir. Saldırgan önceden belirlediği kişileri/kurbanları hangi alanlarda kullanacağını tespit edip bu kişilere karşı bir güven zinciri tesis etmeye çalışacaktır.[29]

25 Social Engineering: Understanding and Auditing - GSEC Practical Assignment – a.g.e

26 Fighting Social Engineering - a.g.e

27 Fighting Social Engineering - a.g.e

28 Aaron Dolan–Social Engineering-GSEC-http://www.sans.org/reading_room/whitepapers/engineering/social_engineering_manipulating_the_source_32914

29 Social Engineering: Understanding and Auditing - GSEC Practical

f) Elektronik posta bazlı denetim

Sosyal mühendisler kurbanlarını istismar etmek için hazırladıkları virüs yazılımlarını çalışanların elektronik postalarına göndermek suretiyle saldırılar düzenlenmektedir. Çalışanların şüphesini çekmeyecek şekilde ustaca hazırlanmış elektronik postalar gönderilerek veya başkalarına zarar vermek amacıyla kurulmuş web sitelerine girilmesi sağlanarak virüslerin bilgisayarlara yüklenmesiyle saldırılar gerçekleştirilmektedir.[30]

Telefon bazlı denetim tekniğinde tanımlanan tekniklerin aynısını uygulayıp, sosyal mühendislerin elde etmek istediği bilgileri ulaşmaya çalışabiliriz. Bu tür denetimlerde öncelikle saldırganların ne çeşit elektronik postaları kimlere gönderdiğini araştırıp, daha sonra hedeflediğimiz çalışanlara aynı kalıpta elektronik postalar göndererek tepkilerini değerlendirmemiz faydalı olacaktır.[31]

Sonuç

Değer ifade eden her türlü bilginin saldırı hedefi haline geldiği günümüzde, çoğu kişi veya kurum sosyal mühendislik saldırılarının hedefi olduğu için çeşitli risklerle karşı karşıya kalmaktadırlar. Hiçbir bilgisayar sistemi insandan bağımsız olmadığı gibi, insan unsuru da güvenlik sisteminin en zayıf halkasıdır. İnsan unsurunun yer aldığı bir sistem içinde sosyal mühendislik saldırılarına karşı bilgisayar güvenlik sistemlerinin kesin güvence sağladığı söylenemez. Bu nedenle sosyal mühendisler, güvenlik zincirinin en zayıf halkasını oluşturan insan unsuruna odaklanıp kurumların savunma mekanizmalarını etkisiz hale getirmeye çalışmaktadırlar.

Sosyal mühendislik saldırılarına karşı açıklıkları tam olarak kapatabilecek savunma yöntemi bulunmamakla birlikte, riskleri hafifletip zararları minimize edebilecek en etkili savunma yöntemi eğitim ve öğretimdir. Bu nedenle eğitim ve öğretim faaliyetleriyle personelin sosyal mühendislik olaylarına karşı bilinçlendirilmesi, çalışanların yaptıkları işin bir parçası olarak güvenlik politikalarından haberdar olmaları ve politika kurallarını uymaları önem kazanmaktadır. Ayrıca denetimlere gereken önemin verilmesi, düzenli denetimler sayesinde zayıflıkların tespit edilerek daha iyi politikaların geliştirilmesi ve güvenlik politikalarının sürekli güncellenmesi en ideal korunma yöntemidir.

Assignment – a.g.e

30 Social Engineering: Understanding and Auditing - GSEC Practical Assignment – a.g.e

31 Fighting Social Engineering - a.g.e

KAYNAKLAR

1. Social engineering attacks: What we can learn from Kevin Mitnick - Mark T. Edmead - 11.18.2002 http://searchfinancialsecurity.techtarget.com/tip/0,289483,sid185_gci1294530,00.html
2. Social Engineering: Understanding and Auditing - GSEC Practical Assignment - By Chris Jones – 4/11/2003 http://www.sans.org/reading_room/whitepapers/engineering/understanding_and_auditing_1332
3. Fighting Social Engineering - Mikael Hermansson & Robert Ravne - University of Stockholm / Royal Institute of Technology - March 2005 http://dsv.su.se/en/seclab/pages/pdf-files/2005-x-281.pdf
4. The Threat of Social Engineering and Your Defense Against It http://www.sans.org/reading_room/whitepapers/engineering/the_threat_of_social_engineering_and_your_defense_against_it_1232?show=1232.php&cat=engineering
5. A Proactive Defence to Social Engineering http://www.sans.org/reading_room/whitepapers/engineering/511.php
6. "Social Engineering" http://www.hq.nasa.gov/office/ospp/securityguide/V1comput/Social.htm
7. Bilgisayar Ağlarında Güvenlik Politikalarının Uygulaması - Ar. Gör. Enis Karaarslan, Abdullah Teke, Prof. Dr. Halil Şengonca http://csirt.ulakbim.gov.tr/dokumanlar/BilgisayarAglarindaGuvenlikPolitikalarininUygulanmasi.pdf
8. Güven Şeker - İnternette Bilişim Suçlarında Kullanılan Metotlar - İzmir İl Emniyet Müdürlüğü http://uretim.meb.gov.tr/EgitekHaber/s75/b%C4%B1ls%C4%B1m%20suclar%C4%B1.htm
9. Can Bican - Sosyal Mühendislik Saldırıları http://www.bican.net/2008/05/20/sosyal-muhendislik-saldirilari/
10. Aaron Dolan - Social Engineering - GSEC Option 1 version 1.4b - February 10, 2004 http://www.sans.org/reading_room/papers/download.php
11. Social Engineering - The Weakest Link in Information Security - Jeff Mc Dermott http://www.windowsecurity.com/whitepapers/Social-Engineering-The-Weakest-Link.html