Gazi Üniv. Müh. Mim. Fak. Der.
Cilt 26, No 1, 89-103, 2011

J. Fac. Eng. Arch. Gazi Univ.
Vol 26, No 1, 89-103, 2011

KURUMSAL BİLGİ GÜVENLİĞİNDE GÜVENLİK TESTLERİ VE ÖNERİLER

Yılmaz VURAL* ve Şeref SAĞIROĞLU**
***** TURKSAT A.Ş Konya Yolu 40. Km.Gölbaşı / Ankara
******Bilgisayar Mühendisliği Bölümü, Mühendislik Fakültesi, Gazi Üniversitesi, Maltepe 06570, Ankara
yvural@turksat.com.tr, ss@gazi.edu.tr

(Geliş/Received: 22.03.2010; Kabul/Accepted: 26.07.2010)

ÖZET

Kurumsal bilgilerin güvenliğinin sağlanmasında, kullanılan bilgi sistemlerinin zafiyetlerin erken teşhisi ve kısa sürede giderilmesi önemlidir. Saldırı gelmeden önce güvenlik zafiyetleri tespit edilerek giderilmesini sağlayan güvenlik testleri kurumsal bilgi güvenliğinin sağlanması açısından büyük önem taşımaktadır. Yüksek seviyede kurumsal bilgi güvenliğinin sağlanması için güvenlik testlerinin tanımı ve hangi amaçla kullanıldığının kurumlar tarafından bilinmesi ve uygulanması gereklidir. Güvenlik testleri, kurumların ihtiyaçları doğrultusunda, belirli bir yöntem ve disiplin çerçevesinde etik kurallara saygılı güvenlik uzmanları tarafından yapılması gerekmektedir. Literatür incelendiğine, kurumsal bilgi güvenliği konusunda kapsamlı ve güncel bilgilerin bulunmadığı, çalışmaların tüm kavramları kapsamadığı, pek çok bilginin ise güvensiz ve ticari web sitelerinden sunulduğu, olanların ise kısa tanımlamaları ve açıklamaları sunduğu belirlenmiştir. Bu çalışmada, kurumsal bilgi güvenliğinin sağlanmasında önemli bir role sahip olan güvenlik testleri ile standartlar ve kılavuzları geliştiren kurumlar kapsamlı olarak sunulmuştur. Sonuç olarak, bu çalışmanın güvenlik farkındalığını arttıracağı, yeni çözüm önerilerinin geliştirilmesi ve uygulanmasını kolaylaştıracağı, sunulan önerilerin hayata geçirilmesiyle de yüksek seviyede kurumsal bilgi güvenliğinin sağlanmasına katkılar sağlaması beklenmektedir.

Anahtar kelimeler: Bilgi güvenliği, kurumsal bilgi güvenliği, bilişim güvenliği, güvenlik testleri, sosyal mühendislik, güvenlik tes standartları.

SECURITY TESTS AND SUGGESTIONS FOR ENTERPRISE INFORMATION SECURITY

ABSTRACT

Diagnosing vulnerabilities in enterprise information systems and recovering them in short time are very important for enabling enterprise information security. Security tests are used to find out security vulnerabilities of the systems before having any attack to and also crucial for securing enterprise information security. Providing high level information security for enterprises, security tests need to be well known and applied to systems. These tests are achieved by security experts according to the needs of enterprises, methods and ethics. When the literature was reviewed on enterprise information security, it has been encountered that compherensive and up-to-date studies were not available, the studies presented not covering all concepts, most of the studies were delivered by commercial and nontrustworty web sites, and also only covering short desciriptions and explanations about them. In this study, security tests, standards and institutions, of which have very important roles in providing better enterprise information security, have been presented in details. As a result of this study, security awareness might be increased, security issues might be applied and managed easily, and applying the tests and suggestions proposed in this article might also help to improve the security for enterprises.

Keywords: Information security, enterprise information security, IT security, security tests, social engineering, security test standards.

1. GİRİŞ (INTRODUCTION)

Bilgi teknolojileri sürekli gelişen ve değişen bir yapıda olduğundan, bilgi güvenliğinin bir defaya mahsus sağlanması veya yapılandırılması kurumsal bilgi sistemleri açısından yeterli değildir. Kurumsal bilgi güvenliğinin sağlanabilmesi amacıyla bilgi güvenliği yaşayan bir süreç olarak ele alınmalı, sistemler güncellenmeli, eğitimler alınmalı, oluşabilecek yeni riskler karşısında yatırımların zamanında ve doğru bir şekilde yapılması gerekmektedir. Ayrıca tüm bu evrelerde güvenlik seviyesinin istenilen düzeyde sağlanıp sağlanamadığının saptanması, varsa mevcut zafiyetleri açığa çıkarmak, açık kapıları bulmak, uygulanan kurumsal bilgi güvenliği politikalarında yeni açıklar olup olmadığını anlamak amacıyla belirli zaman dilimlerinde sistemlerin gözden geçirilmesi gerekmektedir.

Kurumsal bilgi sistemlerinin güvenliğinin sağlanmasında zafiyetlerin erken tespitinin önemi büyüktür. Saldırı gelmeden önce güvenlik zafiyetlerinin tespit edilerek giderilmesini sağlayan güvenlik testleri kurumsal bilgi güvenliğinin sağlanması açısından büyük önem taşımaktadır. Güvenlik testlerinin sınıflandırılarak kurumların ihtiyaçları doğrultusunda, belirli bir yöntem ve disiplin çerçevesinde etik kurallara saygılı güvenlik uzmanları tarafından yapılması güvenlik testlerinin başarılı olması için önemlidir. Bu testlerin amacı kurumsal bilgi sistemlerine düzenlenebilecek saldırıları, saldırgan gözüyle kontrollü olarak saldırı gelmeden önce kontrollü saldırılar düzenleyerek gerekli tedbirlerin önceden alınmasında kurumlara yardımcı olmaktır.

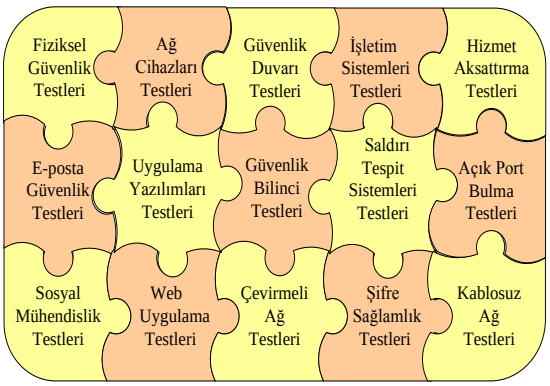
Kurumsal bilgi sistemlerinin güvenliği sadece teknik önlemlerin alınmasıyla sağlanamaz. Teknolojik sebeplerden kaynaklanmayan konularda bilgi sistemlerinin güvenliğini tehdit etmektedir. Güvenlik testleriyle sınanan bilgi sistemleri teknik (bilişim sistemleri, doküman yönetim sistemleri, süreç analizleri, vb.) ve teknik olmayan (çalışanların bilinci, kurum kültürü, yönetimsel prosedürler, fiziksel güvenlik vb.) etkenler dikkate alınarak bir bütün olarak değerlendirilmelidir. Güvenlik testleri değişen risklere paralel olarak periyodik zaman aralıklarında tekrarlanmalıdır. Tekrarlama zaman dilimi kurumların riskleri dikkate alınarak belirlenmelidir.

Kurumsal bilgi güvenliğinin sağlanmasında önemli bir role sahip olan, ülkemizde bu alanda kullanımı çok yaygın olmayan güvenlik testleri konusunda bu çalışmada kapsamlı bir araştırma yapılmıştır. Yapılan incelemelerde öncelikle literatürdeki mevcut tanımlar gözden geçirilmiştir. Daha sonraki bölümlerde güvenlik testlerinin amaçları, sınıflandırılması, kapsamı ve sınırları, standartlar, kullanılan yaklaşımlar, test teknikleri, test aşamaları ve test aşamalarında kullanılan araçlar sırasıyla açıklanmıştır.

2. GÜVENLİK TESTLERİ (SECURITY TESTS)

Güvenlik testleri bilgisayar sistemlerinin güvenliğini değerlendirmede kullanılan en eski yöntemlerden birisidir. 1970'lerin başında A.B.D Savunma Bakanlığı, daha güvenli sistemler oluşturmak için yazılımların geliştirilmesindeki ve bilgisayar sistemlerindeki güvenlik zafiyetlerinin gösterilmesinde bu yöntemi kullanmıştır. "Bilişim sistemlerinde sızma testi" kavramı 1995 yılında geliştirilen ve ilk Unix tabanlı ilk zafiyet tarama sistemi olan "SATAN" programıyla birlikte kullanılmıştır [1].

Genel bir fikir vermesi amacıyla güvenlik testleri Şekil 1'de verilmiştir.



Şekil 1. Güvenlik testlerinin yap-boz gösterimi (Illustrating security test as a puzzle) [52]

Güvenlik testlerinin şematik gösterimi bir yapboz şeklinde tarafımızdan bu çalışma kapsamında ifade edilmiştir. Bu gösterimin amacı güvenlik testlerine bir bütün olarak bakılması, içlerinden herhangi birinin yapılmaması veya düzgün olarak yapılmaması durumunda kurumsal bilgi güvenliğini zafiyete uğratacağından bu testlerin tamamlayıcı olduğunu vurgulamaktadır. Bu yüzden şekilsel olarak dikkat çekici olması için bu çalışma kapsamında yapboz gösterim tercih edilmiştir.

Literatürde güvenlik testleriyle ilgili yapılan tanımlardan önemlileri aşağıda özetlenmiştir.

- Bilgisayar ağı ve ağ kaynaklarındaki zafiyetlerin tespit edilerek bilgi sistemlerinin güvenlik seviyesini değerlendirmek üzere hazırlanan testlerdir. Çoğu zaman etik amaçlı saldırılar (Ethical Hacking) olarak da adlandırılır [2].
- Açık kapı bulma sanatıdır [3].
- Bilgisayar ağlarının güvenliğini artırmak, yeni zafiyet ve sömürüleri ortaya çıkarmak, bilgi sistemlerinin ne derece güvende olduğunu anlamak üzere yapılan testlerdir [4].

- Kurum veya kuruluşların güvenliğini sağlamak amacıyla gerçek dünyadaki saldırı ve saldırgan mantığıyla bilgi sistemlerinin ne derece güvende olduğunu anlamak üzere bilgisayar ağlarına yetkisiz erişim sağlamak için yapılan testlerdir [5].
- Yetkili kişiler tarafından bilinen zafiyetlerin sistematik ve planlı olarak kullanılmasıyla bilgi kaynaklarına (uygulamalar, bilgisayarlar, bilgisayar ağları ve bileşenleri) yapılan kontrollü saldırılardır [6].
- Bilgi güvenliği ölçümlerinin yapılmasını sağlayan bir yöntemdir [7].
- Saldırganların yapabileceğine benzeyen kötücül saldırılar yapılarak bilgisayar sistemlerinin ve ağlarının güvenliğinin değerlendirilmesi yöntemidir [8].
- Güvenlik danışmanları (Ethical Hacker) tarafından sistem veya ağ üzerinde saldırganların hangi tür açıkları tespit edebileceği ve açıklara dayalı bilgilerle neler yapabileceklerinin görülmesi amacıyla yapılan güvenlik testleridir [9].
- Bilgisayar ağları üzerinde saldırganların beceri ve teknikleri kullanılarak, var olan zafiyetlerin uzak konumlardan bulunması amacıyla ağların taranması, tarama sonuçlarının incelenmesi, var olan zafiyetlerin kötüye kullanılması ve son olarak zafiyetin giderilmesi amacıyla yapılan güvenlik testleridir [10].
- Bilgi varlıklarının (uygulamalar, bilgisayar ağları, bilgisayar sistemleri) güvenlik durumunu değerlendirmek için zafiyet, yapılandırma hataları, zayıflıklar yönünden saldırgan teknikleri ile analiz edilmesi sürecidir [11].
- Kurumlar tarafından saldırılar ve yetkisiz erişimlerden bilgisayar sistemlerinin nasıl korunacağıyla ilgili zafiyetlerin değerlendirilmesinde kullanılan ortak bir yoldur [12].
- Koruma sistemlerinin sahip olduğu zafiyetlerin gösterilmesi amacıyla yapılan sızmalardır [13].
- Teknik donanımlı ehil kişiler tarafından yapılan sistematik testlerdir [14].
- Sızma testlerinin amacı güvenliğin test edilmesi olup, kurumsal bilgi sistemlerinin kırılması olarak algılanmamalıdır [15].
- Güvenli Hesaplama Esaslarının (TCB) güvenlik seviyesinin değerlendirmede kullanılan yöntemlerden bir tanesidir [16].

Yukarıda yapılan tanımlar dikkate alındığında, bu çalışma kapsamında kişisel tanımımızı şu şekilde yapabiliriz. Kurumsal bilgi varlıklarının (bilişim sistemleri, insan faktörü, iş süreçleri) zafiyetlerinin saldırgan gözüyle ortaya çıkarılarak giderilmesi amacıyla belirli zamanlarda, yazılımlar, donanımlar ve insanlar üzerinde işinin ehli bir ekip tarafından yapılan etik testlerdir.

3. GÜVENLİK TESTLERİNİN AMAÇLARI (OBJECTIVES OF SECURITY TESTS)

1974 yılında Paul A. Karger ve Roger R. Schell tarafından yazılan "zafiyet analizi", 1975 yılında Richard R. Linde tarafından uluslararası bir konferansta sunulan "işletim sistemleri ve sızma testleri" isimli bildiriler literatürdeki bu konuyla yapılmış ilk çalışmalardır [17]. O günden bu güne, kurumsal bilgi güvenliğinde güvenlik testlerinin kullanımı ve önemi gün geçtikçe artmaktadır. Yapılan bu testlerin ortak amacı, kurumsal bilgi varlıklarına ait güvenlik tehditlerinin (zayıflıklar, zafiyetler, yapılandırma hataları, vb.) kötü niyetli saldırganlardan önce belirlenerek gerekli güvenlik önlemlerinin kurumlar tarafından alınmasına yardımcı olmaktır.

Güvenlik testlerinin amacı kötü niyetli kişilerin yetkisiz erişimlerini engellemek amacıyla zafiyetlerin tanımlanarak giderilmesidir [18]. Güvenlik testleri kurumlar tarafından çok çeşitli amaçlar için pek çok alanda kullanılmaktadır. Bu testler;

- Yeni zafiyetlerin bulunması,
- Tasarım zafiyetlerinin belirlenmesi,
- Güvenilir kurum imajının korunulması,
- Bilgi güvenlik politikalarının gözden geçirilmesi,
- Bilgi güvenliği sertifikasyonlarına uyumda sürekliliğin sağlanması,
- Etkili ve bilinçli güvenlik yatırımının yapılması,
- Güvenlik yatırımlarının geri dönüşümünün mümkün olduğunca yüksek olması,
- Teknik personelin sorumluluğunun gözden geçirilmesi,
- Kurumsal bilgi sistemlerine yapılabilecek olan muhtemel saldırı veya saldırılara karşı güvenliğimizi sürekli olarak yüksek seviyede sağlamak

amaçlı yapılmaktadır. Yukarıda maddeler halinde açıklanan güvenlik testlerinin amaçları takibeden alt başlıklarda sırasıyla açıklanmıştır.

3.1. Yeni Zafiyetlerin Bulunması (Finding New Vulnerabilities)

"Güvenlik satın alınacak bir ürün değil devamlılık gerektiren bir süreçtir" yaklaşımı güvenlik dünyasında kabul görmüş bir yaklaşımdır [19]. Bu yaklaşım güvenliğin sadece bir defaya mahsus olarak başlangıçtaki zafiyetler dikkate alınarak sağlanmasının yeterli olmayacağı, bu sürecin dinamik olduğunu ve güvenliğin sürekliliğinin sağlanmasının önemini vurgulamaktadır. Kurumsal ihtiyaçların her geçen gün artması ve değişmesine bağlı olarak yeni teknolojiler ve yeni yaklaşımların kullanılmasıyla birlikte sistemler ilk kurulduğu andaki zafiyetlerden çok daha fazlasını içermektedir.

Güvenliğin yüksek seviyede sağlanabilmesi için bilgi güvenliği yaşam döngüsünde kullanılan yeni teknolojilerin veya yeni saldırı yöntemlerinin beraberinde getirdiği yeni zafiyetlerin güvenlik testleriyle bulunması ve önlemlerin önceden alınması gerekmektedir. Bilgi yaşam döngüsü boyunca meydana gelebilecek yeni zafiyetlerin (kurtçuklar, işletim sistemi açıkları, virüsler, protokol açıklıkları, personel, vb.) tespit edilememesine bağlı olarak güvenlik ihlalleri yaşanacak ve kurumlar zarar görecektir.

3.2. Tasarım Zafiyetlerinin Tanımlanması (Defining Design Vulnerabilities)

Bilgi sistemlerinde kullanılacak yazılımların tasarımlarının veya bilgi sistemlerinin yerleşeceği fiziksel mekanların tasarımları yapılırken tasarımcılar çoğunlukla güvenlik gereksinimlerini atlamakta veya gereken önemi vermemektedirler. Yazılımların tasarlanması aşamasında tasarımcı programa dış dünyadan yapılacak erişimleri en aza indirgemeli ve dış dünya ile temasta olan kısımların güvenliğinin yüksek seviyede sağlanmasına yönelik bir tasarım ortaya koymaya özen göstermelidir. Bunu takiben dış dünyadan yapılacak olan veri girişlerinin kodlayıcılar tarafından yeterince doğrulanmaması sonucunda zafiyetler oluşacaktır.

İlk bakışta fark edilmesi zor olan tasarım kaynaklı kusurları içeren zafiyetler ancak güvenlik testleriyle ortaya çıkarılabilecektir. Tasarım zafiyetlerinden dolayı başlangıçta güvenli olduğu varsayılan bilgi sistemleri çeşitli saldırılara maruz kalabilmekte ve büyük kayıplar yaşanabilmektedir.

Tasarım zayıflıklarından kaynaklanan zafiyetlere bir başka örnek ise fiziksel ağ tasarımları yapılırken ağ bileşenlerinin (router, switch, hub, kablo, panel, fiber optik kablo sonlandırıcıları) fiziksel güvenliğin (kilitsiz dolaplar, kilitsiz odalar, vb.) yeterince ciddiye alınmamasıdır. Bu tasarım zayıflığına bağlı olarak yetkisiz kişiler ağ aktif cihazları üzerinden bilgilere yetkisiz olarak erişebilecek ve bilgi güvenliği ihlallerinin yaşanmasına sebebiyet verecektir. Bu tasarım zayıflığından kaynaklanan zafiyetlerin kullanılması durumunda ağ yönlendiricisinin saldırıya uğraması (hack edilmesi), verilerin dinlenmesi, hizmetin durması gibi ciddi saldırılar meydana gelebilecektir.

Mantıksal ve fiziksel tasarımlardan kaynaklanan zafiyetlerinin güvenlik ihlallerine dönüşmeden önce güvenlik testleriyle tespit edilerek önlemlerin alınması kurumsal bilgi güvenliğinin yüksek seviyede sağlanması açısından önemlidir.

3.3. Güven Sağlanması (Enabling Trust)

Güvenilir kurum imajı, elektronik ortamlarda iş yapan kurum ve kuruluşların en büyük sermayelerinden birisidir. Müşteri sayısının artması ve mevcut müşterilerin korunması ancak ve ancak "güven" veya "güvenirlik" duygusunun sürekliliğidir.

Elektronik ortamlarda kurumların bu imajını sağlamlaştırmaları için saldırıya uğramadan veya zafiyetlerle karşılaşılmadan önce önlemler alarak, maddi ve manevi kayıpları engelleyebilirler. Bunun için ise güvenlik testleri önemli bir yer tutmaktadır.

3.4. Bilgi Güvenlik Politikalarının Oluşturulması (Establishing Information Security Policy)

Bilgi güvenlik politikalarının oluşturulmasında, kurumsal bilgi sistemlerinin güvenliğini tehlikeye atan tehditler güvenlik testleriyle tespit edildikten sonra risk değerlendirmeleri ve risk analizleri yapılır. Risk analiz sonuçları kurumsal bilgi güvenliği politikaları içerisinde yer alan prosedürler ve standartların oluşturulması için yapılan çalışmalara teknik bir dayanak oluşturur.

3.4. Sertifikasyonlar (Certifications)

Güvenlik testleri kurumsal bilgi güvenliği sertifikasyonlarının alınması için çoğunlukla yapılması zorunludur. Kurumsal bilgi güvenliği yönetim sistemlerinin oluşturulması ve işletilmesi adımlarında kurumsal bilgi varlıklarına ait güvenlik risklerinin tespiti ve analizi çalışmalarına yardımcı olması amacıyla güvenlik testlerinin uygulanması ve sonuçlarının değerlendirilmesi standartlar tarafından zorunlu tutulmuştur.

3.5. Güvenlik Yatırımları (Security Investments)

Güvenlik yatırımlarının doğru ve zamanında yapılması ile ilgili olarak birçok kurum ve kuruluş problem yaşamaktadır. Özellikle ticari kaygısı olan firmaların yanlış yönlendirmeleriyle yetersiz veya gereğinden çok fazla ürünler satın alınmakta dolayısıyla doğru yatırımlar yapılamamaktadır. Buna ek olarak güvenliğin sadece bazı yatırımlar yapılarak sağlanabileceği düşüncesini taşıyan yöneticilerin ikna edilebilmesi de yatırımlar konusunda yaşanan bir diğer zorluktur.

Örneğin bir güvenlik duvarı ve antivirüs yazılımlarının satın alınmasıyla güvenliğin tamamen sağlanacağını düşünen birçok yönetici hatta teknik personel olduğu bilinmektedir. Ancak gerçekte bilgi güvenliğinin sağlanabilmesi için bu çözümlere ek olarak, ağ ve host tabanlı IDS/IPS (Intrusion Detection / Prevention Systems) kişisel bilgilerin gizliliğinin sağlanması için gerekli olan koruma sistemleri, e-posta temelli antivirüs yazılımları, içerik filtreleme, spam posta filtreleme, casus yazılım engelleme ve eğitim gibi yatırımların da yapılması gerekmektedir.

Güvenlik yatırımlarının doğru yapılmaması, yapılsa bile yanlış yapılandırılmasından kaynaklanan zafiyetler güvenlik testleriyle tespit edilebilir. Güvenlik testlerinin sonucunda ortaya çıkan bilgiler gerekli güvenlik yatırımlarının doğru, etkili ve ölçülü bir şekilde yapılması konusunda yöneticilere ve teknik sorumlulara yardımcı olacaktır. Ayrıca güvenlik yatırımlarının doğru yapılmasının bir diğer sonucu ise yatırımın geri dönüşümüdür [20]. Güvenlik testleri sayesinde doğru güvenlik yatırımları yapılması kurumların maddi ve manevi anlamda kâr etmelerini, saygınlığının, itibarının ve güvenilirliğinin artmasını sağlayacaktır.

3.6. İnsan Faktörü (Human Factors)

Bilgi güvenliğini en üst düzeyde tehdit eden ve güvenlik kontrollerinin aşılmasını sağlayan önemli risklerin başında insan faktörü gelmektedir. Örneğin teknik personelin verimliliğinin ve yaptığı işin kalitesinin ölçümlenmesi güvenliğin sağlanması için önemlidir. Çalışanlar bilgi eksiklikleri ve çalışma motivasyonlarının düşük olmasından kaynaklanan, bilerek veya bilmeden önemli hatalar yapmaktadırlar.

Düzenli olarak yedek alınmaması veya alınan yedeklerin test ortamlarında sınanmamış olması, bilgi sistemlerinin üretim esnasında verilen varsayılan (default) şifre ve yapılandırmalarla kullanıma alınması, yayınlandığı halde yazılımlara ait güncelleme ve yamaların yapılmaması, güvenlik yazılımlarındaki kural hataları, gereksiz servislerin kapatılmaması, imza tabanlı güvenlik yazılımlarının veritabanlarının güncel tutulmaması gibi kusurlar insan faktöründen kaynaklanan hatalara örnek olarak gösterilebilir [21]. Güvenlik testleriyle insan faktöründen kaynaklanan hatalar zamanında tespit edilerek gerekli önlemlerin alınması sağlanabilir.

4. GÜVENLİK TESTLERİNİN SINIFLANDIRILMASI (CLASSIFYING SECURITY TESTS)

Güvenlik testlerinin sınıflandırılabilmesi için dikkate alınan kriterler; test başlangıç bilgisi, bilgi sistemleri üzerinde oluşturduğu etkiler, teste yaklaşım yöntemleri, testte kullanılan yöntemler (teknik, teknik olmayan) ve testin yapılacağı yer olarak sıralanabilir.

Kurumların istek ve ihtiyaçları doğrultusunda ve belirlenen kriterleri temel alarak, hangi türde güvenlik testlerinin yapılması gerektiği ilgili güvenlik uzmanları tarafından kararlaştırılır. Kriterler ve test seçenekleri Çizelge 1'de verilmiştir. Bilgi ve yetki, system etkisi, kapsam, yaklaşım, konu ve yöntemler başlıkları altında bu kriterler açıklanmıştır.

Çizelge 1. Güvenlik testlerinin sınıflandırılması (Classifying security tests)

Kriterler	Test Seçenekleri		
Bilgi ve Yetki	Yok	Kısıtlı	Detaylı
Sisteme Etkisi	Pasif	Normal	Aktif
Kapsam	Genel	Sınırlı	Özel
Yaklaşım	Gizli	Açık	Karma
Konum	Kurum dışı	Kurum içi	Karma
Yöntem	Teknolojik	Teknolojik olmayan	Karma

4.1. Bilgi ve Yetki (Information and Authorization)

Güvenlik testleri uzman kişilerden oluşan test takımları tarafından yapılmaktadır. Test takımının güvenlik testi uygulanacak kurum hakkında başlangıç bilgisi üç farklı düzeyde olabilir. Eğer test başlangıcında kurumsal bilgi sistemleri hakkında test takımına hiç bir bilgi ve yetki verilmemişse kara-kutu, bir çalışanın sahip olduğu ölçüde sınırlı bir bilgi ve yetki verilmişse gri-kutu, kurumsal bilgi sistemlerinin tamamı hakkında bilgi ve yetki verilmişse beyaz-kutu testi olarak adlandırılır [22].

Kara-kutu testlerde, test takımı kurumla ilgili bilgileri kamuya açık alanlardan (internet, dergi, kitap, gazete, vb.) çeşitli bilgiler (kurumun web sayfasının adı, kullandığı IP adres aralıkları, vb.) toplar. Sonrasında bu bilgileri anlamlandırarak test için gerekli aşamalarda kullanır. Gri-kutu testlerde, test takımı bir kurum çalışanı ile aynı bilgi ve haklara (kurumun geçmişi, kurumsal kültür, fiziki mekânlara erişim, kullanıcı adı ve şifresi, vb.) sahiptir. Beyaz-kutu testlerde, test takımı bilgi sistemleri hakkında üst derece bilgilere (iş-akışı, doküman yönetim sistemi, işletim sistemlerinin listesi, veritabanı yazılımı platformları, bilgisayar ağı haritası, aktif cihazlar, güvenlik duvarı bilgileri vb.) sahiptir.

4.2. Sistem Etkisi (System Effect)

Güvenlik testleri yapılırken sistemler üzerinde etkilerinin önceden planlanması gereklidir. Testlerin sistemlere olan etkisini pasif, normal ve aktif olmak üzere 3 seviyede sınıflandırabiliriz Pasif testlerde, port ve zafiyet tarayıcıları gibi yazılımlarla elde edilen zafiyetler sadece raporlanır. Normal testlerde, tespit edilen zafiyetlerin tanımlanması ve kullanılması, zayıf parolaların tespiti ve kırılması, bellek taşması gibi yöntemler kullanıldığından sistemlerde bazı anlarda kısa süreli aksamalar veya yavaşlamalar meydana gelebilir.

Aktif testler, elektronik ortamda verilen hizmetlerin aksamasını veya durmasını sağlayan hizmet aksattırma testleri (denial of service), kötü amaçlı yazılımların çalıştırılması (trojan, worm, virüs, vb.), web sayfalarının değiştirilmesi, veritabanı içindeki bilgilerin değiştirilmesi veya silinmesi, yönlendiricilerin çökertilmesi gibi tamamen bir saldırganın yapabileceği tüm saldırıları içerir. Aktif testler uygulanmadan önce tam yedekler alınmalı ve

sistemlerin sanal bir kopyası çıkarılmalıdır. Kurumlar açısından çok kritik olan bilişim sistemlerine ait sızma testleri çalışan sistemlerin bire bir aynısı olan sanal kopyaları üzerinde uygulanması gerekmektedir.

4.3. Kapsam (Scope)

Güvenlik testlerinde kapsam belirlenirken sistemlerin en az zarar görmesi, iş sürekliğinin sağlanması gibi nedenlerden dolayı testlere sınırlamalar getirilmelidir. Sızma testlerine getirilecek olan sınırlamalar, planlama aşamasında aşağıda örnekleri verilen sorulara kurumlar tarafından verilen cevaplara göre yapılmalıdır. Bunlardan bazıları;

- Testler mesai saatlerinde mi veya mesai saatleri dışında mı yapılacak?
- Hizmet aksattırma saldırıları düzenlenecek mi?
- Sistemler üzerinde arka kapılar (truva) yüklenmesine izin verilecek mi?
- Kayıt dosyaları silinecek mi?
- Testlerden çalışanlar haberdar olacak mı?
- Sosyal mühendislik testleri yapılacak mı? Eğer yapılacaksa hangi teknikler kullanılacak?

olarak verilebilir.

Kurumsal bilgi varlıklarının hangilerinin test edileceği, testin amacına uygun olarak belirlenen kapsamlar çerçevesinde oluşturulur. Güvenlik testleri ilk defa yapılıyorsa kurumsal bilgi varlıklarının tamamının kapsam içine alınması, kurumsal bilgi güvenliğinin genel bir değerlendirilmesinin yapılması açısından önemlidir. Test kapsamları genel, sınırlı ve odaklı olmak üzere üç farklı grupta incelenebilir. Bunlar aşağıda kısaca açıklanmıştır.

Genel kapsam içerisinde; kurumların tüm bilgi varlıklarına ek olarak, bilgi alışverişinde bulunulan kurumlar, iş ortakları, danışmanlık alınan firmalar test kapsamı içerisine dâhil edilir. Bu kapsamı seçen kurumların amacı kurumsal bilgi trafiklerinin tamamının denetlenerek kurumun genel bir güvenlik resminin çıkartılması ve güvenlik seviyelerinin ne düzeyde olduğunun belirlenmesidir. Bu ilk kez yapılacak güvenlik testleri için uygun bir yaklaşımdır.

Sınırlı kapsam içerisinde; kurum tarafından belirlenen alan veya alanlar dikkate alınarak testler yapılır. Merkez binaların test edilmesi, bilişim ortamlarının test edilmesi gibi genele göre daha sınırlı alanların test edilmesi sınırlı kapsama örnek olarak gösterilebilir. Sınırlı kapsamda amaç çok geniş ölçekli kuruluşlarda kurumsal bilgi varlıklarının parçalara ayrılarak sırasıyla test edilmesi esasına dayanır.

Odaklanmış kapsam; kurumlar açısından kritik olan ve iş süreçlerini birinci derecede etkileyen bilgi varlıklarının derinlemesine ve dikkatlice test edilmesini içerir. İnternet erişim firmaları için erişilebilirliği, bankalar için bütünlüğü, askeri kurumlar için bütünlük ve gizliliği etkileyen faktörlerin göz önüne alınarak kapsamın belirlenmesi odaklanmış kapsama örnek olarak verilebilir.

4.4. Yaklaşım (Approach)

Güvenlik testlerinin gerçekçi sonuçlar vermesi için testlerin bazı aşamalarında gizlilik bazı aşamalarında şeffaflık önemlidir. Güvenlik testlerinin uygulanmasında testlerin gizliliği, test sonuçlarının doğruluk oranını önemli derecede etkiler. Çalışanların güvenlik bilincinin gerçek anlamda ölçülebilmesi, kendilerinden bilgi almak isteyen test ekip üyesi hakkında bilgi sahibi olunmamasına bağlıdır.

Önemli sunucuların performansını düşürecek, beklenmedik hatalar oluşturacak ve geri dönüşü olmayacak şekilde kayıplara sebebiyet verebilecek testlerin uygulanmasında ise şeffaflık testlerin sonucunda meydana gelebilecek istenmeyen sonuçların en aza indirgenmesi veya kısa zamanda telafi edilebilmesi için önemlidir. Örneğin; sunucular ve üzerinde çalışan servisler test edilirken, sistem yöneticisinin bu testlerden haberinin olması ortaya çıkabilecek olumsuz durumlarda olaylara acil bir şekilde müdahaleye hazır olması gereklidir.

4.5. Konum (Location)

Kurum içinden veya kurum dışından yapılan sızma testleri, testlerin konumunu belirler. Kurum içinden yapılan testler, iyi niyetli olmayan kullanıcılar veya kurum içerisinde sızmış yerel saldırganlar (internal hacker) tarafından kullanılabilecek olası zafiyetlerin ortaya çıkarılmasını sağlar. Kurum dışından yapılan testlerde ise dış dünyadan gelebilecek tehditler ve zafiyetlerin belirlenmesi hedeflenmektedir. Kurum dışından yapılan testlerde test ekibinin başlangıçtaki bilgisi dış dünyadaki bir saldırgana eşdeğerken, kurum içinden yapılan testlerde ise test ekibi başlangıçta bilgi sistemleri hakkında detaylı bir bilgiye sahiptir. Kurum içinden yapılan testlere örnekler aşağıda verilmiştir [23]. Bunlara;

- Yetkisiz olarak bilgi kaynaklarına erişme ve bu kaynakları kullanma,
- Yerel alan ağ mimarisinin belirlenerek ağ topolojisinin oluşturulması,
- Ağ cihazlarının yapılandırılmasının değiştirilmesi,
- Web sayfasının değiştirilmesi,
- Güvenlik duvarı kurallarının atlanması (by-pass),
- Yetki seviyesinin değiştirilmesi,
- Yerel alan ağındaki bilgilerin dinlenmesi ve değiştirilmesi,
- Çalışanlar adına e-posta atılması,
- Antivirüs yazılımlarının sistemden kaldırılması,
- Parola kırma testlerinin yapılması,
- Sunucu dayanıklılık (stres) testleri,

- Fiziksel olarak yapılan erişim ihlâllerinin test edilmesi ve
- Kurum içi bilgi güvenliği farkındalık testleri (sosyal mühendislik)

gibi örnekler vermek mümkündür.

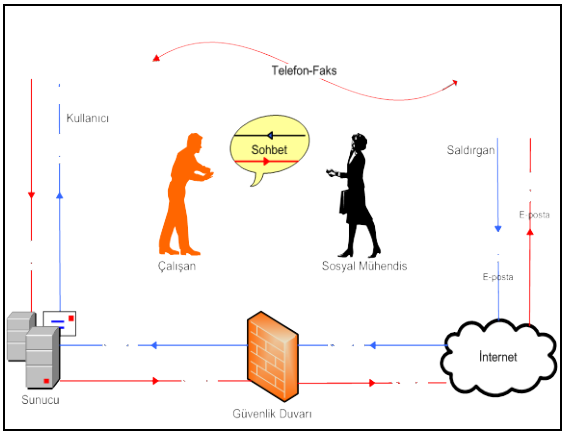
Günümüzde yapılan araştırmalardan ve yayınlanan raporlardan [24–31] saldırıların büyük bir kısmının yerel saldırganlar tarafından kurum içerisinden yapıldığı belirtilmektedir. Kurum içindeki bir saldırganın verebileceği zararları tespit etmek (kurum içi sızma testleriyle) kurumsal bilgi güvenliğinin üst seviyede sağlanması açısından büyük önem taşımaktadır.

Kurum dışından yapılan güvenlik testlerinde ise genellikle; güvenlik güncellemeleri yapılmamış, güvenlik programları yanlış yapılandırılmış, güvenlik dikkate alınmadan geliştirilmiş web uygulamaları, kullanıcıların bilmedikleri ama cazip başlıklı e-postalar (spam, phishing, hoax, vb.), bilgi ve bilinç eksikliğinden kaynaklanan insan hatalarının araştırıldığı sosyal mühendislik testleri karşısında çalışanların davranışlarının ortaya çıkartılması, gibi kurumsal bilgi güvenliğini doğrudan etkileyecek unsurlar üzerinde yoğunlaşılmaktadır.

4.6. Yöntemler (Methods)

Güvenlik testlerinin uygulanmasında kullanılan yöntemler teknik ve teknik olmayan olmak üzere iki grupta incelenmektedir. Teknik olmayan testler insan faktöründen kaynaklanan zafiyetlerden faydalanılarak kurumsal bilgi varlıkları hakkında bilgi ve belge toplamak için yapılan testlerdir. Teknik olmayan testlerin başında sosyal mühendislik (social engineering) testleri gelmektedir. Sosyal mühendislik (toplum mühendisliği), yalan söyleme ve ikna etme üzerine kurulan inandırma ve bilgi toplama sanatıdır [32]. Sosyal mühendislik testlerinden sonuç alabilmek için farklı yöntemler kullanılmaktadır. Bu yöntemlerden en çok kullanılanı telefon yoluyla taklit ve ikna yöntemidir. Sosyal mühendisliğin başarılı olabilmesi için testi yapan kişilerin, ikna ve taklit yeteneği yüksek, her türlü cevaba ve soruya kendini hazırlayan, hazır cevap, ses tonuyla kişiler üzerinde olumlu etkiler bırakan, kendini iyi pazarlayan, ikna edici senaryo yazan, kişilerin zafiyetlerinin farkında olan, iyi derecede iletişim kabiliyetine sahip insanlar olmalıdır. İnsan-makine, makine-makine, insan-yazılım, yazılım-yazılım, korsan-karma (makine, yazılım, insan) arayüz ortamları sosyal mühendislik vakaların yaşanabileceği muhtemel ortamlardır.

Şekil 2'de sosyal mühendislik tek bir resim içerisinde temsili olarak gösterilmektedir. İlk yöntem olarak, saldırgan bilgisayar başından hazırladığı sazan postalarla kullanıcıyı kandırmakta ve istediği bilgilere ulaşabilmektedir. İkinci bir yöntem ise saldırgan farklı bir iletişim ortamı olan telefon veya faks cihazları üzerinden yapılan kandırmacalarla istediği bilgilere ulaşabilmektedir. Sosyal mühendislik testlerinin en etkili yöntemlerinden birisi olan üçüncü yöntemde ise sohbet ortamlarında, sosyal mühendis sohbet ortamlarında hissettirmeden istediği bilgilere karşısındaki insanı yönlendirici konuşmalar yaparak ulaşmaktadır. Sosyal mühendisler genellikle bakımlı, iyi giyimli, şık, konuşması düzgün karşısındaki insanı etkileyeci bir görünüme sahiptirler.



Şekil 2. Sosyal Mühendislik Temsili Gösterimi (Illustrating social engineering) [52]

Sosyal mühendislik testlerinde kullanılan diğer bir yöntem ise çöplük karıştırma (dumpster diving) diye tabir edilen testlerdir. Kurumların kırtasiye çöplerinde bulunabilecek ve tam anlamıyla imha edilmemiş dokümanlar üzerinde geçerliliğini yitirmemiş bilgiler sayesinde kurumlar hakkında önemli bilgilere ulaşılabilir. Kırtasiye atıklarıyla ilgili olarak kurumlar tarafından yapılan hatalara örnek olarak, ortak kullanıma açık olan yazıcılarda çıktıların karışmaması için kullanıcının ismi, dokümanların adının yazılı olduğu ve genellikle çıktı sahibi tarafından direkt olarak çöpe atılan kâğıtlar vardır. Bu kâğıtlar sayesinde kurumun kullanıcı profili ve üzerinde çalıştığı konu başlıkları hakkında fikir sahibi olunabilir. İkinci örnek olarak, aynı dokümanın çalışma sonuçlanıncaya kadar çok defa çıktısı alınır ve her defasında üzerinde değişiklik yapılarak bir önceki kopya çöpe atılır. Ancak, çöpe atılan dokümanlar hala geçerliliğini korumakta ve yapılan çalışmalar hakkında detaylı bilgiler içermektedir. Üçüncü örnek olarak, küçük notların yazıldığı ve üzerinde genellikle önemli hatırlatıcı bilgilerin yer aldığı küçük kâğıtlar üzerine yazılı bilgi notları vardır. Bu bilgi notları telefon numaraları, adresler, toplantı notları, kullanıcı adı ve şifreleri içerebilir.

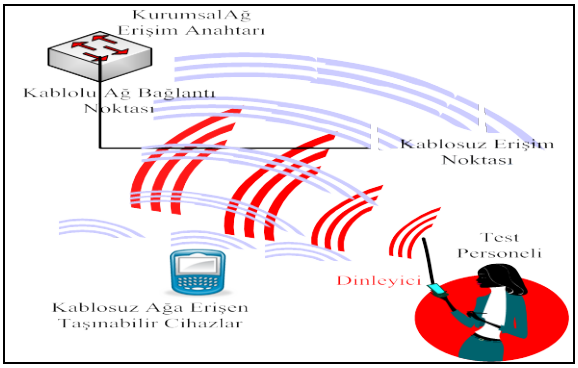
Sosyal mühendislik testlerinde kullanılan diğer bir yöntem ise masaüstü testleridir. Kişilerin masalarında

bıraktığı ve herkes tarafından kolaylıkla okunabilecek bilgi notları, açık bırakılan bilgisayar ekranları, evrakların kilitli olmayan ortamlarda muhafaza edilmesi sonucunda kurum ve kişiler açısından çok değerli bilgiler rahatlıkla elde edilebilir. Masaüstü testleri, çalışanlar masasında otururken ve masasından ayrıldıktan sonra yapılabilir. Çalışanlar masadayken göz ucuyla civarda veya masa üzerinde bulunan bilgi notlarına bakmak, şifresini bilgisayara girerken gözetlemek (omuz sörfü), çalışanların masadan uzaklaşmasıyla parola korumalı ekran koruması olmayan bilgisayara girmek, kilitli olmayan dolapları açmak şeklinde yapılabilir.

Teknik testler için özel olarak geliştirilmiş yazılımlar ve donanımlar kullanılarak yapılan testlerdir. Teknik testler kurumlara ve teknoloijlere özgü olarak geliştirilen testler olduklarından bu çalışmada en çok bilinen testlerden bazıları açıklanmıştır.

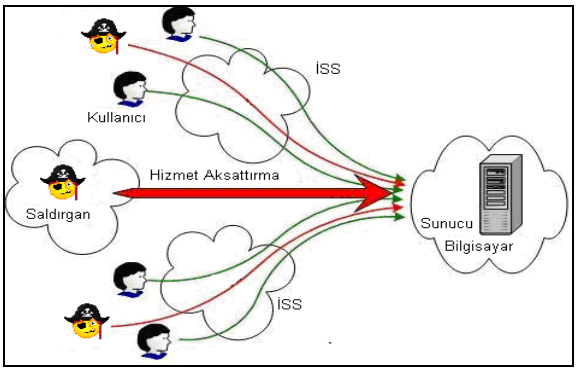
Teknik testlerden birincisi bilgiye yetkisiz olarak erişim yapabilme amacını taşıyan pasif dinlemelerdir. Dinlemeler yoluyla kullanıcı sistemleri (terminal, iş istasyonları, telefonlar, veri hatları, vb.) ile merkezi sistemler (sunucular, internet servis sağlayıcıları, vb.) arasında akan iletişim trafiği yetkisiz olarak izlenebilmektedir. Bu testler aracılığıyla bu tür tehditlerin etkisini en aza indirgemek için gerekli olan önlemlerin alınması sağlanmaktadır. Dinleme, farklı iletişim ortamlarında gerçekleştirilebilir. Bunlardan birincisi bakır teller üzerindeki iletişim trafiğinin dinlenmesidir. Asenkron, senkron veya kiralık bakır hatlar üzerinde akan trafiğin herhangi bir noktadan paralel olarak hatta girilmesiyle dinlenebilme imkânı vardır. İkinci dinleme ortamı ise yerel alan ağları üzerindeki paketlerin dinleyici yazılımlarla bir kopyasının alınmasıdır. Sunucu bilgisayara bağlanmak üzere sisteme giriş yapan bir kullanıcının, kullanıcı adı ve şifresi bu teknikle ele geçirilebilir. Üçüncü dinleme ortamı, güvenli olarak bilinen fiber optik kablolarda yapılır. Fiber kabloların dışındaki koruyucu tabaka soyulup U biçiminde kıvrılarak kıvrılan yerden gerekli ışık çoğaltılarak fiber kablo üzerinden geçen trafik dinlenebilir. Dördüncü dinleme ortamı Şekil 3'de gösterilen kablosuz ortamlardır. Kablosuz ortamlarda çalışan, bilgisayarlar kablosuz ağ ortamları için geliştirilmiş olan dinleyici yazılımlar yardımıyla dinlenebilir.

Teknik testlerden ikincisi, erişim kontrollerinin ihlal edilebilirliğinin ölçümlenmesidir. Bu testler vasıtasıyla kullanıcı adları ve şifreler kaba kuvvet teknikleri (brute force) veya akıllı tahminlerle elde edilebilirliği ölçümlenmektedir. Kaba kuvvet testleri güçlü bilgisayarlar kullanılarak bütün olasılıkların değerlendirilmesi esasına dayanır [33]. Akıllı tahmin adı verilen testlerde çok kullanılan şifre ve kullanıcı adlarını barındıran veri tabanlarından faydalanılır.



Şekil 3. Kablosuz ortamlarda dinleme [52]

Teknik testlerden dördüncüsü, Şekil 4'de gösterilen hizmet aksattırma testleridir [34]. Bu testlerle bir sisteme düzenli olarak yapılan saldırılar sonucunda hedef sistemin hizmet veremez hale gelmesi veya o sisteme ait tüm kaynakların tüketimi amaçlanmaktadır. Hizmet aksattırma testleriyle bir veya daha fazla noktadan bilgi sistemleri üzerine gereğinden fazla yükler bindirilerek, sistemler üzerindeki asli hizmetlerin aksaması ve bu aksama anında zayıflayan sistemlere sızılabilirlik ölçümlenmektedir. Disk alanlarının doldurulması, işlemci tüketimi, yerel alan ağlarındaki merkezi anahtarlara trafik yüklemek, internet yönlendiricilerine gereksiz trafik yükleyerek yetkisiz erişim elde etmek, hizmet aksatma testlerinden bazılarıdır.



Şekil 4. Hizmet Aksattırma (Denial of Service) [52]

Teknik testlerden dördüncüsü, yazılım ve donanımlarda var olabilecek zafiyetlerin ortaya çıkarılmasıdır. Bu zafiyetlere örnek olarak bellek taşmaları, işletim sistemi, uygulama yazılımı, kodlama ve yapılandırma zafiyetleri örnek olarak gösterilebilir. Teknik testler daha da arttırılabilir ancak bu çalışma kapsamında en çok genellikle kurumların tamamına yakını tarafından uygulanabilecek yöntemlere yer verilmiştir.

5. GÜVENLİK TESTLERİNİN YAPILMASI (APPLICATIONS FOR SECURITY TESTS)

Güvenlik testleri planlama, bilgi toplama, zafiyetlerin bulunması, zafiyetlerin kullanılması, raporlama olmak

üzere beş aşamada gerçekleştirilirler [35]. Bu aşamalar takibeden alt başlıklarda sırasıyla açıklanmıştır.

5.1. Planlama (Planning)

Planlama; kapsam tespiti, test türleri, zaman dilimleri, riskler, araçlar, personel, işin süresi, maliyet, etik, bilgi değişimi ve gizlilik anlaşmaları konularını içeren başlangıç aşamasıdır. Kapsam, güvenlik testlerinin yapılmasına karar verildikten sonra ihtiyaçlar doğrultusunda Bölüm 4.3'te bahsedilen kapsamlardan birisine karar verilir. Test türünde ise Bölüm 4.6'da anlatılan testlerden hangileri yapılacağına dair kararlar verilir. Riskler, uygulanacak olan testlerin hangi riskleri taşıdığına dair bilgiler test ekibi tarafından mevcut açıklıklar dikkate alınarak belirlenerek testi yaptıracak kuruma bildirilir. Bazı testler ve bu testlerin uygulanması sonucunda ortaya çıkabilecek olan risk seviyeleriyle ilgili bilgiler Çizelge 2'de gösterilmiştir.

Çizelge 2. Testler ve Risk Seviyeleri (Tests and Risc Levels)

Testler	Risk Seviyesi
Sosyal Mühendislik	Orta
Hostların Keşfedilmesi	Düşük
Kullanılan Portların Keşfedilmesi	Düşük
Kullanılan Servislerin Tespiti	Düşük
Otomatik Zafiyet Tarama	Orta
Çevirmeli Ağ Tarama (Wardialing)	Düşük
Kablosuz ağlarda Tarama (Wardriving)	Düşük
Parola Kırma	Orta
Zafiyetlerin İstismarı	Yüksek
Hizmet Aksattırma Testleri	Orta

Testlerde kullanılan araçlar, yazılımlar (bilgi toplama yazılımları, zafiyet tarama yazılımları, programlama dilleri, vb.) veya donanımlar (telefon, faks, ağ dinleme cihazları, bilgisayar, vb.) olabilir [36].

Güvenlik testlerinin başarılı bir şekilde yapılabilmesi için ekip çalışmasına ihtiyaç vardır. Bu ekip içerisinde teknik yönden ileri düzeyde bilgi sahibi olması gereken kişilerin yanında ve sosyal yönü gelişmiş, insanlarla iyi iletişim kurabilen ikna kabiliyeti yüksek kişilere de ihtiyaç vardır. Ayrıca ekip içerisinde koordinasyonu sağlayan, planlamayı yapan, test sonuçlarını yorumlayan ve raporların yazılmasını sağlayan bir koordinatöre ihtiyaç vardır [37].

Süre, güvenlik testlerinde belirlenen kapsama bağlı olarak değişir. Kapsam genişledikçe test edilecek bilgi varlıklarının sayısının artmasına bağlı olarak süre ve maliyet artışı olur.

Planlama tamamlandığında; kurumsal bilgi varlıklarının tespit edildiği, tespit edilen bilgi varlıklarının sınıflandırıldığı ve güvenlik testinin omurgasının oluşturulduğu bilgi toplama aşamasına geçilir.

5.2. Bilgi Toplama (Information Harvesting)

Bilgi toplama aşamasında test tipine bağlı olarak, kamuya açık ortamlarda yapılan aramalar yoluyla kurumların bilgi sistemleri üzerinde araştırmalar yapılır. Bu araştırmalarda test konumuna (kurum içi, kurum dışı) göre açık kaynaklar (internet, intranet, gazeteler, haber grupları, dergiler, televizyonlar, vb.) ve sosyal mühendislik testleriyle kurum veya kuruluşlar hakkında detaylı bilgiler toplanır. Sızma testleri sonucunda kurum içinden ve kurum dışından toplanabilecek bilgilere ait örnekler Çizelge 3'de verilmiştir.

Kurumlar hakkında bilgi toplanabilmesi için internet büyük bir fırsat sunmaktadır. İnternet üzerinden yapılan alan adı sorgulamaları kurumlar hakkında birçok bilginin elde edilmesini sağlamaktadır.

Bilgi toplamada en çok başvurulan ikinci yöntem arama motorlarıdır. Arama motorları içerisinde bilgiye ulaşımda Google arama motoru ön plana çıkmaktadır. Google arama motoru kullanarak gizli bilgilere ve zafiyetlere ulaşılabilmesine "Google Hack", arama motorunda kullanılacak olan ifadeleri içeren veritabanıda "Google Hack Veri Tabanı (GHDB)" olarak adlandırılmaktadır [38]. Sızma testlerinde arama motorları hem kamuya açık bilgilere, hemde web yöneticilerinin yapılandırma hatalarından kaynaklanan güvenlik açıkları sayesinde gizli bilgilere ulaşmakta kullanılmaktadır. Bilgi toplamada kullanılacak diğer bir yöntem, etki alanı isim çözümleme sunucularının (DNS) sorgulanmasından elde edilen teknik bilgilerdir. Bilgi toplamada kullanılacak başka bir yöntem ise daha önceki bölümde detaylı şekilde açıklanmış olan sosyal mühendislik veya toplum mühendisliği yöntemleridir. Sosyal mühendislik yöntemleriyle ikna kabiliyetine bağlı olarak önceki yöntemlerde bahsedilen birçok bilgiye ve daha fazlasına ulaşmak mümkün olabilmektedir.

5.3. Zafiyet Analizi (Using Vulnerabilities)

Zafiyet, saldırganların sömürebileceği hatalardır [39]. Bilgi kaynakları (insan, haberleşme, bilgisayar ağları, bilgisayar, vb.) üzerinde var olan ve istismar edilebilecek güvenlik boşluklarının tespit edilmesi, tanımlanması ve sınıflandırılması süreci zafiyet analizi olarak adlandırılmaktadır [40]. Bilgisayarlar ve ağlar üzerindeki zafiyetlere ek olarak bu sistemlerin işletilmesiyle ilgili politika ve prosedürlerden kaynaklanan zafiyetlerde bu kısımda tanımlanır. Bu çalışmada zafiyet, bilgi sistemlerinde gizlilik, bütünlük ve erişilebilirlik faktörlerinden en az birinin ihlâl edilmesini sağlayan kusurlar olarak tanımlanmıştır. Sosyal mühendislik, politika, prosedür eksikliklerinden kaynaklanan zafiyetler insanları etkilerken, mantıksal yazılım hataları veya tasarım

zayıflıklarından kaynaklanan zafiyetler ise sistemleri etkilemektedir [41].

Çizelge 3. Bilgi Toplama (Information Harvesting)

Konum/ Yöntem	Toplanabilecek Bilgiler
İnternet (Kurum Dışı)	İletişim Bilgileri (Web, Posta Adresi, Tlf, Faks, E-posta)
	Alan İsimleri
	Dış Dünyaya Açık IP Bloğu
	IP'lerin Sunucularla (Güvenlik Duvarı, Web, DNS, E-posta, vb.) Eşleştirilmesi
	Yazılımların ve İşletim Sistemlerinin Tespiti
	Ağ Geçidinin Belirlenmesi (Yönlendirici)
	Güvenlik Yazılımlarının Tespiti (Güvenlik Duvarı, Saldırı Tespit Sis., vb.)
	Uzaktan Erişim Protokollerinin Keşfedilmesi (VPN, Remote Desktop)
İntranet (Kurum İçi)	Kullanılan Ağ Protokolleri (IP, DHCP, DNS, NAT, vb.)
	Dâhili Alan İsimleri Yapılandırması
	Dâhili Ağ IP Bloklarının Belirlenmesi
	Ağ Topolojisinin Belirlenmesi
	Erişim Kontrol Listeleri Mekanizmalarının Tespiti
	Dâhili Saldırı Tespit Sisteminin Keşfedilmesi
	Uygulama Yazılımları Platformlarının Belirlenmesi (.Net, Java)
	Veri Tabanlarının Belirlenmesi
	Sunucu Bilgisayarların Belirlenmesi ve Görevlerinin Tespiti
	Güvenlik Yazılımlarının Tespiti
Sosyal Mühendislik (Kurum İçi-Kurum Dışı)	Telefon Yoluyla Taklit ve İkna
	E-posta Yoluyla Kandırmaca
	Çöplük Karıştırma
	Masaüstü Testleri
	Fiziksel Erişim

Zafiyet analizi yapılırken izlenen basamaklar:

- Kaynakların tanımlanması ve sınıflandırılması, ve önem seviyelerine göre önceliklendirilmesi,
- Her bir kaynak için potansiyel tehditlerin belirlenmesi,
- Önemli görülen potansiyel problemlerle ilgili güvenlik stratejilerinin geliştirilerek gerekli önlemlerin alınması ve
- Eğer saldırı başarılı olursa meydana gelebilecek kötü sonuçların en aza indirgenebilmesi için yapılması gerekenlerin tanımlanması

olarak sıralanabilir.

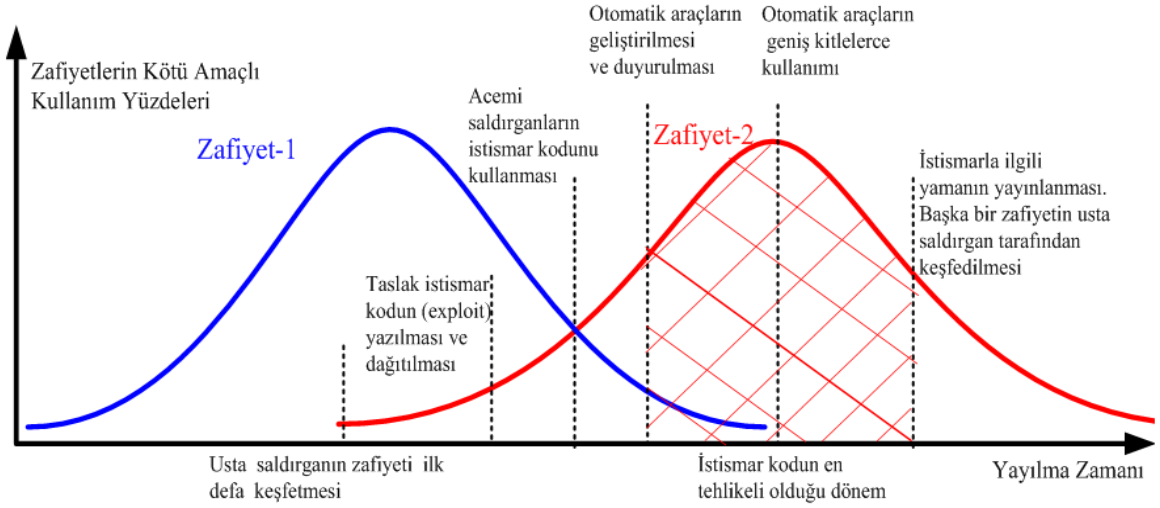
Güvenlik testlerinin uygulanacağı kurumsal bilgisayar ağlarında, zafiyet analizlerinin yapılabilmesi için ağa bağlı cihazlar (bilgisayar, yönlendirici, anahtar, vb.) üzerindeki açık portların belirlenmesi, işletim sistemleri ve çalışan uygulamaların (sürüm numarası, yama seviyesi, servis paketleri, vb.) tespit edilmesi gerekmektedir. Günümüzde zafiyet analizlerinin yapılmasını sağlayan zafiyet tarayıcıları olarak da adlandırılan otomatik yazılımlar vardır. Bu yazılımlar içerisinde bulunan veri tabanlarında daha önceden duyurusu yapılmış mevcut zafiyet tanımları yer almaktadır. Veri tabanına kayıt edilmemiş ve yeni bir zafiyetin keşfedilmesi açısından otomatik yazılımlarla yapılan zafiyet analizlerine ek olarak manüel yöntemlerle yapılan zafiyet analizlerinin yapılması da gerekmektedir. Zafiyet analizleri sonucunda daha önce duyurulmamış yüksek seviyeli tehditler içeren güvenlik boşlukları bulunduğunda, yazılım ve donanım üreticilerine güvenlik boşluğuyla ilgili bilgi verilmesi ilgili yamaların çıkartılması açısından önemlidir.

5.4. Zafiyetlerin Kullanımı (Vulnerability Uses)

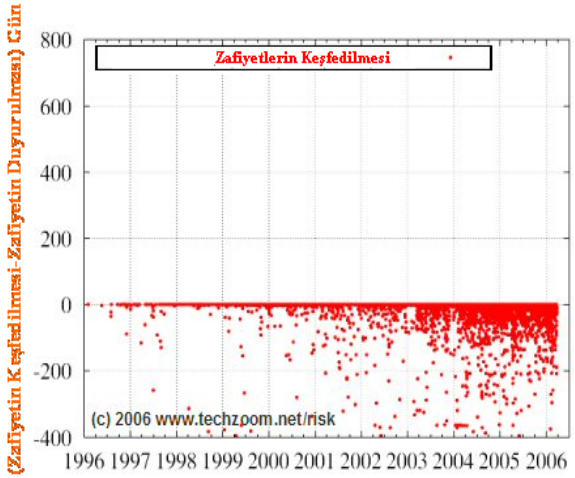
Zafiyetlerin kullanımı güvenlik testlerinin en önemli aşamasıdır. Bilgi sistemleri üzerinde bulunan yazılımlara ait güvenlik açıklarının kullanılmasını sağlayan küçük programlar istismar kodları (exploit) olarak adlandırılmaktadır [42]. İstismar kodları zafiyetlerin genel veya özel kullanımı için farklı programlama dillerinde (C, C++, Perl, Lisp, Python, vb.) uzman yazılımcılar veya usta saldırganlar tarafından geliştirilmektedir. İstismar kodları bilgi sistemlerine olan erişim haklarına göre uzak (remote) ve yerel (local) olmak üzere iki sınıfa ayrılırlar. Sızma testi yapılacak sunucu bilgisayar üzerinde daha önceden verilmiş erişim hakkı yok ise "uzak", erişim hakkı var ise "yerel" istismar kodları olarak adlandırılmaktadır. "Kara-kutu" testlerde (erişim hakkı olmayan) sistemlere erişim sağlanabilmesi amacıyla uzak istismar kodları kullanılırken, "Beyaz-kutu" testlerde (erişim hakkı olan) sınırlı yetkilere sahip kullanıcı hesabına ait erişim hakkının yükseltilebilmesi için yerel istismar kodları kullanılmaktadır. Zafiyet ve istismar kodları arasındaki ilişki grafik olarak Şekil 5'de gösterilmiştir.

Güvenlik açığının keşfedilmesini takiben geliştirilen istismar kodları sıfır gün istismar kodları olarak adlandırılmaktadır [43]. Güvenlik yamaları yayınlanana kadar sıfır gün istismar kodları tüm bilgi sistemlerini tehdit etmektedir. Sıfır gün istismar kodları Şekil 6'da gösterildiği gibi hızlı bir şekilde artmaktadır. Saldırganlar tarafından oluşturulan sıfır gün istismar kodlarının hızlı bir şekilde artması sızma aşamalarında kullanılan mevcut istismar kodlarına ek olarak yeni istismar kodlarının geliştirilmesi ihtiyacını doğurmuştur.

İstismar kodlarının yazılabilmesi, test edilebilmesi amacıyla ticari ve açık kaynak kodlu çerçeve yazılımlar geliştirilmiştir. 2006 yılında insecure.org sitesi tarafından en çok kullanılan yüz güvenlik aracının belirlenmesi için yapılan ankete 3,243 kişi katılmıştır. Zafiyet kullanım araçları isimli kategoride açık kaynak ve ticari programlar değerlendirilmiş ilk üçü Metasploit Framework, Core Impact ve Canvas isimli yazılımlar almıştır. Bunlar aşağıda kısaca tanıtılmıştır [44]. Çizelge 4'de kısaca tanıtılan bu yazılımlar 17 farklı özellik dikkate alınarak karşılaştırılmıştır [45].



Şekil 5. Zafiyet Yaşam Süreci (Vulnerability life cycle) [52]



Şekil 6. Sıfır Gün İstismar Kodları (Zero-day exploits) [51]

Metasploit Framework, istismar kodlarının kullanılması, test edilmesi ve yazılması için komple çözüm sağlayan sızma testlerinde kullanılan ücretsiz (açık kaynak) zafiyet kullanım aracıdır. Bunlar Perl ve Ruby dilinde geliştirilmiştir. Core Impact, ticari amaçlar için geliştirilmiş geniş bir istismar kodu veri tabanına sahip güçlü ve oldukça pahalı bir çerçeve yazılımıdır. Python ve C++ programlama dilinde geliştirilmiştir. Canvas, ImmunitySec firması tarafından ticari amaçlar için geliştirilmiş zafiyet kullanım yazılımıdır. Zafiyetlerin kullanımı aşamasında otomatik çerçeve yazılımların yanında elle (manüel) yapılan kullanımlarda çok önemlidir. Elle yapılan zafiyet kullanımına örnek olarak uygulamalar üzerinde bilinçli olarak, hataların meydana getirilmesi, meydana gelen hatalardan sistem hakkında bilgiler alınması ve alınan bilgilerin yardımıyla zafiyetlerin tespit edilerek kullanılabilirliği test edilmektedir.

5.5. Raporlama (Reporting)

Güvenlik testleri sonucunda verilecek rapor tüm çalışmayı özetleyerek güvenliğin sağlanması için gerekli olan önlemler ve tavsiyeleri içeren, karar verme aşamasında üst yönetime tavsiyeler içeren bir kılavuz niteliğinde olmalıdır [46].

Çizelge 4. Zafiyet Bulan Yazılımlarının Karşılaştırılması (Comparing vulnerability detection software) [45]

Özellikler	Core Impact	Canvas	Metasploit
İşletim Sistemi	Windows	Windows / Unix	Windows / Unix
Grafik Kullanıcı Arabirimi	Var	Var	Var
Betik Dili	Python	Python	V 2.x Perl / V 3.x Ruby
Ağ Haritalama	Var	Var	V 2.x Yok / V 3.x Planlanıyor
Uzak İstismar Kodları	Var	Var	Var
Yerel İstismar Kodları	Var	Var	Yok
Web İstismar Kodları	Var	Yok	Yok
Encoder Kullanımı	Yok	Yok	Var
Ajan Üzerinden Saldırı	Var	Yok	Meterpreter / SocketNinja
Payload Kullanımı	Agent / InlineEgg	Agent	Meterpreter / Shellcode
İstismar Sonrası Bağlantı	Bind/Reverse/Re-use	Bild/ Reverse/ Re-use	Bild/Reverse/FindSock
Otomatik İstismar İşlemi	Var	Var	Yok
Raporlama	Var	Yok	Yok
Diğer Araçlarla Entegrasyon	Var	Var	V 2.x Yok / V 3.x Planlanıyor
Harici Geliştirme Araçları	Yok	Yok	Var
Anti-Forensic Özellikleri	Yok	Yok	Var
Fiyat	27.500TL	3500TL (10 Kul.)	Ücretsiz

Raporun içeriği yönetim özeti, gerçekleştirilen hizmetler ile sonuç ve önerilerin yer aldığı üç ana kısımdan oluşmalıdır. Bunlar kısaca aşağıda açıklanmıştır.

Yönetim özeti, güvenlik testleri sonucunda bulunan olumlu veya olumsuz önemli noktaların yer aldığı, genellikle bir sayfaya sığdırılması istenilen üst yönetim tarafından okunması gereken raporun özet kısmıdır. Üst yönetimin kurumsal bilgi güvenliğinin mevcut durumunu doğru değerlendirmesi açısından bu kısımda güvenliği olumsuz etkileyen noktaların yanında, olumlu noktalarında belirtilmesi zorunludur.

Gerçekleştirilen hizmetler, kısmında testlerle ilgili olarak kapsam, yöntem, kısıtlamalar ve yapılan testlerin detaylarının yer aldığı bu kısım raporun en önemli bölümünü oluşturmaktadır. Testler sonucunda elde edilen ham teknik bilgiler raporun ekinde verilmelidir.

Sonuç ve öneriler kısmında, test sonuçlarının yorumlanarak önerilerin önem derecesine göre sıralanarak kısa, orta ve uzun vadede alınması gereken önlemler ve tavsiyeler yer almalıdır. Ayrıca testler sırasında karşılaşılan güçlükler ve sebepleri bu kısımda gerekçeleriyle birlikte anlatılmalıdır.

6. STANDARTLAR VE KILAVUZLAR (STANDARDS AND GUIDELINES)

Sızma testlerinin yapılmasında kullanılan açık kaynaklı projeler olarak geliştirilen dünyada yaygın olarak bilinen önemli standart ve kılavuzlar takip eden alt başlıklarda kısaca açıklanmıştır.

6.1. OSTMM

Güvenlik testlerinde kullanılan en yaygın rehberlerden birisi olan ve açık kaynak olarak geliştirilen OSSTMM (The Open Source Security Testing Methodology Manual) güvenlik testlerinin ve ölçümlerinin yapılması için oluşturulan çerçeve bir yapıdır [47]. Bu çerçeve yapı ISECOM (The Institute for Security and Open Methodologies) isimli kar amacı olmayan ve Amerika ve İspanya'da faaliyet gösteren bir enstitü bünyesinde geliştirilmektedir. Bu projenin amacı, sızma testlerinin yapılmasında bir model geliştirmek ve bu modele uygun yapılan sızma testlerinin enstitü tarafından onaylanmasını sağlamaktır.

OSSTMM modeline göre sızma testleri; bilgi güvenliği, süreç güvenliği, internet teknolojileri güvenliği, iletişim güvenliği, kablosuz ağ güvenliği ve fiziksel güvenlik olmak üzere altı ana bölümde yapılmaktadır. Her ana test bölümünün kendi içerisinde yapılacak testlerin bulunduğu modüller bulunmaktadır. Bu modüllerin içerisinde ilgili testin nasıl yapılması gerektiğine dair adımlar testlerde kullanılacak taslak dokümanlar, testlerin sonucunda elde edilmesi gereken bilgilerin yer aldığı açıklamalar yer almaktadır. OSSTMM modeline göre ana test alanları ve modülleri aşağıda kısaca açıklanmıştır [48].

Bilgi güvenliği testleri: Bu bölümde sızma testi yapılacak olan kurum hakkında ayrıntılı gözden geçirme ve incelemeler yapılmaktadır. Mevcut durumun değerlendirilmesi, bilgi bütünlüğünün, insan kaynaklarının ve mahremiyet denetimlerinin gözden geçirilmesi bu bölümde yapılan çalışmalardan bazılarıdır.

Süreç güvenliği testleri: Bu bölümde kurumun işleyişine etki eden süreçlerin güvenliği test edilmektedir.

İnternet güvenlik testleri: Test alanları içerisinde en fazla modüle sahip olan bu bölümde 19 farklı test uygulanmaktadır. Bu testler aracılığıyla, ağ ve internet ortamları üzerinde bilgi güvenliğinin test edilmesi amaçlanmaktadır. Ağ haritasının çıkarılması, saldırı tespit sistemlerinin gözden geçirilmesi, sistem servislerinin tanımlanması, internet üzerinden hizmet veren uygulamaların test edilmesi, yönlendirme testleri, erişim kontrolü, şifre kırma, hizmet aksattırma ile güvenlik politikalarının gözden geçirilmesi gibi testlerdir.

İletişim güvenlik testleri: Haberleşme ortamlarının güvenliğinin sağlanmasıyla ilgili testler bu bölümde yapılmaktadır. Genel bir değerlendirmenin arkasından, telefon, faks, modem, sesli posta ve uzaktan erişim gibi iletişim ortamlarına ait testlerdir.

Kablosuz ortam testleri: Kablosuz ortamlar aracılığıyla haberleşen cihazların güvenliği bu bölümde test edilmektedir. Genel bir değerlendirme sonrasında, 802.11x kablosuz ağlarının test edilmesi, bluetooth ağlarının test edilmesi, kablosuz diğer cihazların ve elektromanyetik yayılım testlerini kapsar.

Fiziksel güvenlik testleri: Fiziksel güvenliğin sınanması için kapı giriş ve çıkış sistemlerinin edilmesi, alarm ve izleme sistemlerinin test edilmesi, erişim kontrollerinin test edilmesi bu bölümde yapılan çalışmalardan bazılarıdır.

OSSTMM modeline göre yukarıda açıklanan test alanlarının bir kısmı veya tamamı kurumlara uygulanabilir.

6.2.NIST

Ulusal Standart ve Teknoloji Enstitüsü (National Institute of Standards and Technology-NIST) tarafından geliştirilmiş ve "Ağ Güvenliği Test Rehberi" ismiyle Amerika'da standart haline getirilmiştir. Bu rehber kurumların BT altyapılarını

kendi kendilerine test edebilmeleri ve ağ güvenliklerini sağlayabilmeleri için gerekli olan çalışmaların bir yaşam döngüsünde nasıl yapılacağına dair açıklamaları içermektedir. Bu standart kurumların ağ güvenliğinin test edilmesi için sahip olduğu bilgi teknolojisi altyapısının sistematik bir şekilde incelenip araştırılması konusunda bir metodoloji tanımlamaktadır [49].

6.3.OWASP

Açık kaynak Web Uygulama Güvenliği Projesi (The Open Web Application Security Project-OWASP) güvenli web servisleri ve web uygulamaları geliştirilmesi amacıyla yazılım araçları geliştirilmesini ve kılavuzlar yazılmasını sağlayan açık kaynaklı bir çalışmadır [50]. OWASP aynı zamanda web servisleri ve web uygulamalarının güvenlik testinin yapılması için geniş katılımın sağlandığı topluluklar tarafından yürütülen çalışmalar yapmaktadır. Web uygulama güvenliği, saldırganların web servisleri ve web uygulamalarını hedef haline getirmesiyle daha fazla önem kazanmıştır.

6.4. ISACA

İsviçre Bilgi Güvenliği Derneği'nin bilgi güvenliğiyle ilgilenen özel bir grubu ile ISACA (Information Systems Audit and Control Association) tarafından ortaklaşa yapılan bir çalışma sonucunda "Kaplan Timiyle BT Sistem Güvenliği Testi" adında bir kitapçık yayınlanmıştır. Kaplan takımı kavramı güvenlik testlerini yapan takıma karşılık gelmektedir. Bu kitapçık, güvenlik testlerini tespit etme, önerme ve kontrat, risk analizi, testler ile rapor ve sunum olmak üzere 4 kısımda incelemektedir. Testler bölümü güvenlik testlerinin nasıl yapılacağına dair açıklamaların tanımlandığı bölümdür.

7. SONUÇLAR VE DEĞERLENDİRMELER (RESULTS and CONCLUSIONS)

Kurumsal bilgi güvenliğine etki eden faktörlerin bir bütün olarak saldırgan gözüyle sınanması, zafiyetlerin tespit edilerek giderilmesi için yapılacak düzeltmelerin ve sıkılaştırmaların belirlenmesi, sızma testlerinin bilgi güvenliğinin sağlanmasındaki önemini özetlemektedir. Bilgi güvenliğine etki eden faktörlerin güvenlik testleriyle olan ilişkisi bu çalışma kapsamında elde edilen Şekil 7'de gösterilmiştir. Yüksek seviyede bilgi güvenliğinin sağlanmasında güvenlik testleri süreklilik isteyen bilgi güvenliği üçgeninin merkezinde yer almakta ve bilgi güvenliğinin devamlılığının sağlanmasında önemli rol oynamaktadır.

Güvenlik testleri, çalışan bilgisayar sistemlerinin başına olumsuz bir durum gelmeden önce, sistem açıklarını önleyecek ve alınabilecek karşı tedbirlerin karşı savunulacak ve ihtiyaçların düşünülmesinde kullanılan önemli bir erken uyarı sistemidir. Güvenlik testlerinin başarılı olabilmesi için kurumların güvenliğine etki eden faktörlerinin ağırlıkları dikkate alınarak kuruma özgü farklı senaryolar geliştirilmesi gereklidir. Güvenlik testleri için geliştirilen senaryolar kurumlarda kullanılan teknolojilere, çalışanların bilgi düzeylerine, kurumsal bilgi güvenliği seviyesine, bilgi güvenliği bileşenlerinin dozuna göre farklılık gösterebilir.

Güvenlik testleri, bilgi güvenliği ihlallerinin kontrollü bir şekilde tespit edildiği, kurumsal bilgi güvenliğinin sağlanması için düzenli olarak yapılan askeri tatbikatlara benzetilebilir. Tatbikatlar bir ülkenin güvenliğini sağlayan ordular için ne kadar önemliyse, güvenlik testleride kurumlar için bilgi güvenliğinin sağlanması açısından aynı derecede öneme sahiptir. Tatbikatın başarısı gerçek savaş ortamlarının tam anlamıyla simülasyonuna bağlıyken, sızma testlerinin başarısı da gerçek dünyada bilgi güvenliği için tehditler oluşturan saldırganların teknik ve taktiklerinin tam olarak simülasyonuna bağlıdır. Saldırganlar her geçen gün yeni teknik ve taktikler geliştirerek veya geliştirilmiş araçları kullanarak kurumlara saldırmaktadır. Kurumsal bilgi güvenliğinin sağlanabilmesi için saldırganlarla meydana gelebilecek olası sanal savaşların kazanılması gerekmektedir. Düzenli olarak yapılan güvenlik testleri, eksiklikler, aksaklıklar, zayıflıklar ve ihtiyaçların meydana çıkartılarak sanal savaşların saldırganlara karşı kazanılmasında önemli rol oynayacaktır.

Şekil 7. Güvenlik Testlerinin Önemi (Importance of security tests) [52]

Günümüzde birçok bilgisayar sisteminin güvenlik gereksinimleri göz önünde bulunmaksızın tasarlanmıştır. Bu sistemleri yeniden kurmak çoğunlukla maliyet ve zaman açısından imkânsızdır. Bu sistemler üzerinde yapılacak güvenlik testleri sonucunda zafiyetlerin tespit edilerek güvenlik açıklarının giderilmesi zaman ve maliyet açısından uygun ve istenen bir çözümdür. Bu durum kurumsal bilgi güvenliğinde güvenlik testlerinin maliyet ve zaman boyutları açısından önemini göstermektedir.

Çalışma kapsamında yapılan araştırmalar sonucunda ülkemizde güvenlik testlerinin henüz yaygınlaşmadığı ve kurumlar tarafından kurumsal bilgi güvenliğinin sağlanmasında önemli bir bileşen olduğunun

bilinmediği tespit edilmiştir. Bu durum güvenlik testlerinin kurumlara katkılarının, sağlayacağı farkındalığın ve güvenlik seviyesinin artırılmasına katkısının pek bilinmediğinin ve yeterince önem verilmediğinin göstergesidir. Ülkemizde çok az sayıda olan güvenlik firmalarıyla güvenlik testleri konusunda görüşmeler yapılmış ve izlediği metodolojiler hakkında bilgiler edinilmeye çalışılmıştır. Çoğunluğunun güvenlik testlerini piyasadaki hazır araçlar (zafiyet tarama, port tarama, şifre kırma, vb.) kullanarak yaptıkları tespit edilmiştir. Sadece hazır araçlar kullanılarak iyi bir sızma testi yapılamaz. Doğal olarak, otomatik araçlarla yapılan teknik içerikli sızma testlerinin sonuçları gerçek durumu yansıtmayacaktır. Yüksek seviyede bir bilgi güvenliğinin sağlanabilmesi amacıyla birçok elle yapılan teknik olmayan testlerinde mutlaka yapılması gerekmektedir.

Güvenlik testleri bilgi güvenliği ihlallerinin önceden tespit edilmesini ve bilgi güvenliğinin sağlanmasında aksayan yönlerin ortaya çıkartılmasının bulunmasını sağlayan erken uyarı sistemleri gibi davrandığından kurumsal bilgi güvenliğinin sağlanmasında çok önemli bir yeri olduğu çalışma sonucunda elde edilen önemli bulgulardan birisidir.

Güvenlik testlerinin kurumsal açıdan faydaları değerlendirilmiş olup çok çeşitli amaçlar için aşağıda maddeler halinde verilen alanlarda kullanılması bu çalışma kapsamında kurumsal bilgi güvenliğinin sağlanması açısından önerilmektedir.

- Bilgi sistemlerindeki yeni ve varolan zafiyetlerin bulunması veya tespit edilmesi,
- Bilgi sistemlerindeki güvenlik tasarım zafiyetlerinin belirlenmesi,
- Kurumsal bilgi güvenliğini tehdit eden risklerin varlığının ve derecesinin tespit edilmesi,
- KBG politikalarının oluşturulması,
- Kurumsal itibar ve imaj ve saygınlığın korunması,
- KBG yönetim sistemleri sertifikasyonlarına uyum,
- Etkili ve bilinçli güvenlik yatırımı,
- Güvenlik yatırımlarının geri dönüşümü,
- Teknik personelin verimliliğinin ölçümü,
- İnsan faktörünün istenmeyen yönde devreye girmesine sebep olan bilgi güvenliği farkındalığının ölçümü ile
- Kurumsal bilgi sistemlerine yapılacak olan muhtemel saldırı veya saldırılara karşı güvenlimiyiz sorusunun cevaplanması

gibi çok geniş aralıkta kullanımı ele alınabilir.

Kurumsal bilgi güvenliğine etki eden unsurlar içerisinde en zayıf halka olarak adlandırılan insan faktörünün en tehlikeli güvenlik açığı olarak kabul edilen güvenlik bilinci zayıflığının belirlenmesinde sosyal mühendislik yöntemiyle yapılan güvenlik testleri önemli bir role sahiptir. Her geçen gün teknolojik önlemlerin ilerlemesi yazılım veya donanımdan kaynaklanan güvenlik açıklarının minimize edilmesi nedeniyle saldırganlar, insan zafiyetlerinden faydalanarak saldırılarını gerçekleştirmektedirler. Bu tür saldırıların kurumsal bilgi güvenliğini en az oranda tehdit etmesi amacıyla sosyal mühendislik teknikleri ve önemi her kademede yer alan kullanıcılar tarafından bilinmelidir. Bu çalışmada elde edilen önemli bulgulardan birisi de ülkemizde sosyal mühendislik kavramının henüz tam olarak anlaşılamadığı veya önemsenmediği, kurumların ve çalışanların bu konuda yeterli bilgiye sahip olmadıkları tespit edilmiştir. Bu çalışmanın sosyal mühendislik konusunda da kurumlar ve çalışanlar nezdinde farkındalık yaratması beklenmektedir.

Sonuç olarak, yukarıda yapılan tespitlere ek olarak bu çalışma kapsamında güvenlik testlerinin yapılma yöntemleriyle ilgili geniş bir literatür çalışması yapılmış, yapılan çalışmalar sonucunda, güvenlik testlerinin nasıl yapılacağına dair bir yöntem sunulmuştur. Bu yönteme göre, güvenlik testleri planlama, bilgi toplama, zafiyetlerin bulunması, zafiyetlerin kullanılması, raporlama olmak üzere beş aşamada gerçekleştirilmektedir. Bu yöntemle gerçekleştirilen güvenlik testlerinin yapılmasıyla kurumsal bilgi güvenliğinin yüksek seviyede sağlanmasına önemli bir katkı sağlayacağı değerlendirilmektedir.

KAYNAKLAR (REFERENCES)

1. Federal Office for Information Security "A Penetration Testing Model" ***BSI,*** Bonn, 6-9, 93, 2002.
2. Cole, E., Krutz, R., Conley, J. W., "Security Assessments, Testing, and Evaluation", Network Security Bible, ***Wiley Publishing Inc.***, Indianapolis, 607-612, 2005.
3. Geer, D., Harthorne, J., "Penetration testing: a duet" ***IEEE 18th Annual Computer Security Applications Conference***, Las Vegas, 185, 2002.
4. Budiarto, R., Ramadass, S., Samsudin, A., Noor, S., "Development of Penetration Testing Model for Increasing Network Security", ***IEEE International Conference on Information & Communication Technologies: From Theory to Applications,*** Damascus**,** 563, 2004.
5. Nilsson, J., "Vulnerability Scanners" Yüksek Lisans Tezi, ***Department of Computer and Systems Sciences Royal Institute of Technology***, Stockholm, 28-30, 2006.
6. Braden J., "Penetration Testing – Is it right for you?" ***SANS Institute***, Maryland, 1, 2002.
7. İnternet: Corsaire Limited "What is a Penetration Test?" http://www.penetration-testing.com (21.03.2007).

8. İnternet: Wikipedia "Penetration Test" http://en.wikipedia.org/wiki/Penetration_testing (21.03.2007).

9. Lammle, T., "CEH Certified Ethical Hacker Review Guide", ***Sybex Inc.***, Alameda, 8, 2005.

10. Harris, S., Harper, A., Eagle, C., Ness, J., Lester, M., "Gray Hat Hacking: The Ethical Hacker's Handbook", ***McGraw-Hill Osborne Media***, New York, 73, 2004.

11. Manzuik, S., Gold, A., Gatford, C., "Network Security Assessment from Vulnerability to Patch" ***Syngress Publishing Inc.***, Rockland, 104, 2007.

12. Dautlich, M., "Penetration Testing — the Legal Implications" ***Computer Law & Security Report***, 20(1):41, 2004.

13. Cohen, F., "Managing Network Security — Part 9: Penetration Testing?", ***Network Security,*** 1997(8):13, 1997.

14. Schultz, E., "Hackers and Penetration Testing", ***Network Security***, 1997(10):10, 1997.

15. Midian, P., "Perspectives on Penetration Testing", ***Computer Fraud & Security***, 2002(6):15, 2002.

16. Weissman, C., "Security Penetration Testing Guideline", Handbook for the Computer Security Certification of Trusted Systems, ***Center for Secure Information Technology Naval Research Laboratory***,Washington, 2, 1995.

17. Dahl, M. O., "Using Coloured Petri Nets in Penetration Testing", Yüksek Lisans Tezi, ***Department of Computer Science and Media Technology Gjøvik University***, Gjøvik, 18, 2005.

18. Abrams, D. M., "FAA System Security Testing and Evaluation-Technical Report", ***MTR 02W0000059,*** Virginia, 3-7, 2003.

19. Schneier, B., "The Process of Security", http://infosecuritymag.techtarget.com/articles/april00/columns_cryptorhythms.shtm (21.03.2007).

20. İnternet: Wilson, M., "Demonstrating ROI for Penetration Testing (Part One)" http://www.securityfocus.com/infocus/1715 (22.03.2007).

21. Landwehr, C. E., Bull, A. R., Mcdermott, J. P., Choi, W. S., "A Taxonomy of Computer Program Security Flaws" ***ACM Computing Surveys***, 26(3), 214-215, 1994.

22. Splaine, S., "Testing Web Security-Assessing the Security of Web Sites and Applications", ***Wiley Publishing Inc.***, Indianapolis, 3-4 (2002.

23. Heald, A., E., "Understanding Security Testing" ***Infosec Writers***, 8, 2005.

24. Symantec Corp., "Symantec Internet Security Threat Report Trends for July–December 06" ***Symantec Volume XI,*** Cupertino***,*** 24-64, 2007.

25. Gordon, L. A., Loeb, M. P., Lucyshyn, W., Richardson, R., "CSI/FBI, Computer Crime and Security Survey", ***FBI Computer Security Institute***, 1- 26, 2005.

26. Koç.net Haberleşme Teknolojileri ve İletişim Hizmetleri A.Ş., "Türkiye İnternet Güvenliği Araştırma Sonuçları 2005", ***koc.net, İstanbul***, 5-12, 2005.

27. Üneri, M., "BT Güvenliği Güncel Durum ve Eğilimler", ***TÜBİTAK-UEKAE Kamu Kurumları Bilgi Teknolojileri Güvenlik Günü,*** Ankara 27- 35, 2006.

28. Eriş, M., "Türkiye Kamu Kurumları BT Güvenlik Analiz Sonuçları ve Çözüm Önerileri", ***TÜBİTAK–UEKAE Kamu Kurumları Bilgi Teknolojileri Güvenlik Günü,*** Ankara***,*** 7-9, 2006.

29. Eriş, M., "Kamu Kurumları Bilgi Teknolojileri Güvenlik Günü Anket Sonuçları", ***TÜBİTAK–UEKAE Kamu Kurumları Bilgi Teknolojileri Güvenlik Günü,*** Ankara, 10-32, 2006.

30. The Australian High Tech Crime Centre, "Australian Computer Crime & Security Survey", ***AusCERT,*** Canberra, 12, 2006.

31. National ICT Security & Emergency Response Centre, "Malaysia ISMS Survey", ***NISER-ISMS Survey,*** Kuala Lumpur, 4, 35-40, 2003.

32. Mitnick, K. D., Simon, W. L., "Aldatma Sanatı", Nejat Eralp Tezcan, ***ODTÜ Yayıncılık,*** Ankara, 303, 2006.

33. İnternet: Wikipedia "Brute Force Attack" http://en.wikipedia.org/wiki/Brute_force_attack (22.03.2007).

34. İnternet: Columbia University Computer Science Department "A Distributed Denial of Service Attack" http://nsl.cs.columbia.edu/projects/sos/ (22.03.2007).

35. Northcutt, S., Zeltser, L., Winters, S., Kent, K., Ritchey, W. R., "Inside Network Perimeter Security", ***Sams Publishing***, Indiana, 540-550, 2005.

36. Layton, P. T., "Penetration Studies – A Technical Overview", ***SANS Institute***, Maryland, 3-7, 2002.

37. National Infrastructure Security Co-ordination Centre, "Commercially Available Penetration Testing", ***NISCC-Best Practice Guide,*** London***,*** 24, 2006.

38. Long, J., "Google Hacking for Penetration Testers", ***Syngress Publishing Inc***., Rockland, 135- 137, 2005.

39. Potter, B., McGraw, G., "Software Security Testing" ***IEEE Security & Privacy Magazine***,2(5): 81, 2004.

40. Search Security Definitions, "Vulnerability analysis", http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1176511,00.html (22.03.2007).

41. Knight, E., "Computer Vulnerabilities", ***Artech House***, Boston, 7-9, 2000.

42. Foster, J., C., Liu, V., "Writing Exploits and Security Tools", ***Syngress Publishing Inc.***, Rockland, 16, 2006.

43. İnternet: SearchSecurity Definitions, "Zero-day Exploit", http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci955554,00.html (23.03.2007).

44. Singh, P., Mookhey, K.K., "Metasploit Framework, Part 1" http://www.securityfocus.com/infocus/1789 (23.03.2007).
45. Özavcı, F., "Metasploit Framework ile Güvenlik Denetimi", ***Linux Şenliği ODTÜ***, 4-5, 2006.
46. Tiller, J. S., "A Framework for Business Value Penetration Testing", ***Auerbach Publications***, New York, 288- 291, 2005.
47. İnternet: ***ISECOM*** "The Open Source Security Testing Methodology Manual", http://www.isecom.org/osstmm (23.01.2007).
48. Herzog, P., "OSSTMM 2.2. Open-Source Security Testing Methodology Manual", ***ISECOM OSSTMM 2.2,*** Barcelona, 44, 47, 49, 68, 71, 83, 99-101 2006.
49. Wack, J., Tracy, M., Souppaya, M., "Guideline on Network Security Testing" ***NIST Special Publication 800-42,*** Washington, 1 2003.
50. İnternet: Wikipedia "OWASP" http://en.wikipedia.org/wiki/OWASP (23.03.2007).
51. www.techzoom.net/risk (23.03.2007).
52. Vural, Y., "Kurumsal Bilgi Güvenliği ve Sızma Testleri" ***Yüksek Lisans Tezi***, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, 2007.