Ağ Güvenliği Yaşam Döngüsü

Önder Şahinaslan[1], Mesut Razbonyalı[2], Ender Şahinaslan[3]

[1] Maltepe Üniversitesi, Bilişim Bölümü, İstanbul

[2] Okan Üniversitesi, Mühendislik –Mimarlık Fakültesi, İstanbul

[3] Bankasya, İstanbul

Özet: Gelişen ve küreselleşen insan yaşamında, doğru bilgiye doğru zamanda ve güvenle ulaşılabilmelidir. Ağ ve internet bağlantısı yeni nesil teknolojilerinde aranan özelliklerin başın da gelmektedir. Kablolu ve kablosuz bağlantı şekillerindeki hızlı büyüme farklı güvenlik seviyesinde ki ürünlerin kullanımını gerektirmektedir. Bilginin hedefle kaynak arasında aktarımı sırasında, geçtiği her bir düğüm noktası ve sunucu protokolleri toplam ağ güvenlik riskini doğrudan etkiler. Kurumlar veya bireylerin ağ üzerindeki veri iletimi ve etkileşimi doğrultusunda arada kullanıldıkları güvenlik araçları, kritik risk değeri ve kendi içinde uyguladıkları güvenlik politikaları özelleşebilir. Ancak dünyada kabul görmüş standartlara dayalı bir ağ güvenliğinde izlenilebilecek süreçler bir yaşam döngüsü oluşturmalıdır[1]. Bu çalışmada, ağ güvenliğini yaşayan ve sürekli gelişen bir döngü olarak tasarlanmıştır. Döngüde olması gereken başlıklar belirtilmiş ve bunlara ait belli dönemlerde yapılması gereken güvenlik testinin şekli özetle anlatılmıştır.

Anahtar Sözcükler: Ağ Güvenliği, Sızma Testi, İzleme, Denetim ve Raporlama

Abstract: In developing and global human life, accurate information should be accessible with security and on time. Network and internet connection are most wanted features for new generation technology. Wired and wireless connections require hardware products in different security levels. During transferring information between destination and source, each node and server protocols affect total network security risks. Security tools, critical risk values and in-house security policies can be customized in accordance with the transmission and the interaction of data over the network for institutions or individuals. But network security processes based on worldwide accepted standardslife cycle should be established. [1] In this study, living and constantly evolving network security is designed as a cylce. Entries must be specified through the cylce and the form of security test was briefly explanied belongs to these entries in certain periods.

Keywords: Network Security, Monitoring, Control and Reporting

1. Giriş

Mümkün olan her yerden internet erişimi ve platform üzerinde hizmet veren yazılımlar geliştikçe sosyal ağlar, üyelikler, ve e-işlemler(e-bankacılık, e-ticaret, e-eğitim, e-devlet..) büyük bir iletim ve etkileşim kanalı olmaktadır. Bilişim alanında çığ gibi büyüyen bu sektör üzerinden başta üretici firmalar yatırımlarını artırmakta, kullanıcılardan gelen talepler doğrultusunda da bu kullanım biçimi artarak çeşitlenmektedir. Bilginin kaynağı büyük oranda bir kuruma bağlı, belli sayıda çalışanı ve üyeleri olan sistem içerisinde paylaşılabilmektedir. Dolayısıyla belli sayıda kullanıcısı olan özellikle kurumsal ağlarda, alınması gereken güvenlik tedbirleri ve risk düzeyi çok daha önemlidir. Hızlı büyüyen yapılarda ağın genişlemesi her zaman homojen yapıda olmayıp bazı ihtiyaçlar veya plansız yatırımlar nedeniyle heterojen bir şekilde kurulabilmektedir. Sistematik şekilde tasarlanmayan bu tip durumlarda güvenlik açıklıklarının takibi oldukça güçleşmektedir. Bir ağ kurgulanırken, global rekabet ve uygun fiyat endişesiyle cihazlar üzerlerinde set edilmiş güvenlik yazılımları ve olması gereken fiziksel önlemler istenilen seviyede olmayabilmektedir. Zincirin en zayıf halkası örneğinde olduğu gibi güvenlik bir bütündür. Sunucudan başlayıp ağın diğer ucundaki hatta internetteki son kullanıcının erişimine ulaşılana kadar aradaki tüm yazılım ve donanım ürünleri bu güvenliğin bir parçasıdır. Bir güvenlik başlangıcı üzerinde yönetme ve müdahale edebilme hakkına sahip olunan yerden başlamaktadır. Yani ağ güvenliği denildiğinde kapsamı fiziksel olarak çevrilmiş bir bölge içersinde kalan bilgi varlıkları olarak algılanmamalıdır[2]. Bize ait bir bilginin hedeften kaynağa, iletildiği son noktaya kadar arada kullanılan yazılım ve donanım ürünlerinin tamamını kapsamaktadır.

Öncelikle bilginin kaynağı yani tutulduğu sunucu sistemi buna bağlı yerel ağ bileşenleri ve iç kullanıcıların erişimi güvenli olmalıdır. Saldırı ve zafiyetlerin en çok yaşandığı ve güvene dayalı gözden kaçırıldığı kritik bir alandır. Daha sonra dış bağlantılar yani doğrudan veya dolaylı erişimin yapıldığı oldukça çok boyutlu kompleks yapıdaki erişimin güvenliği sağlanmalıdır.

Bunu yaparken bugüne kadar yapılmış çalışmalar, deneyimler, bilimsel ve akademik literatür çalışmaları ile elde edilen standartlara dayalı bir yöntem takip edilmelidir. Ancak bu şekilde başından sona sistemde her hangi bir noktasında güvenlik zafiyeti bırakmadan planlama yapılabilir. Kurgulanan bu güvenlik döngüsünün yeterli olup olmadığı ancak iyi niyetli yapılacak bir çeşit saldırı testi ile ortaya çıkartılabilir[6].

Bir ağ güvenliği yaşam süreci; kurulumundan itibaren başlayıp belli zaman aralıklarında devam eden sızma testleri ile ortaya çıkabilecek zafiyet risklerinin yönetildiği işlem süreçlerinin bütünüdür. Bu süreç parametrelerinin neler olduğu ve güvenlik test tiplerinin ne şekilde yapılacağı açıklanmıştır.

2. Ağ Güvenliği Gelişim Süreci

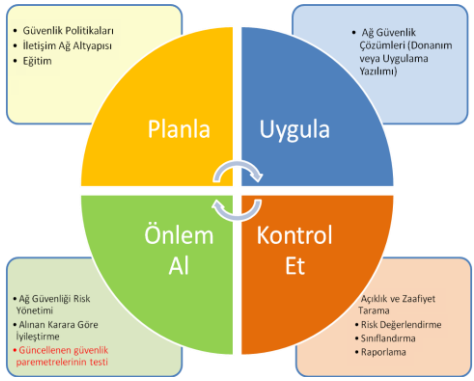
Kişisel bilgisayarlarda üretilen bilgilerin zaman içerisinde farklı bilgisayarlarda ve farklı uygulamalarla paylaşılması ihtiyacı doğmuştur. Bu paylaşım ve iletim teknolojilerdeki gelişmeyle birlikte her geçen gün daha da ihtiyaç haline gelmiştir. Bilgiye anlık ve hızlı erişimle beraber iletimdeki gizlilik, bütünlük ve doğruluk oldukça önemlidir.

Bunun yanı sıra bilgisayar ağlarından beklenen iş türleri de zaman içerisinde çeşitlenerek artmıştır. Bu kullanım en büyük erişim platformu internet ve bunun altyapısını teşkil eden ağlar üzerinden gerçekleşmektedir. Bu büyük potansiyelin karşılanmasına yönelik kurumsal veya bireysel bağlantılar tasarlanıp kurulurken bilginin korunması uluslar arası ölçekte düşünülmelidir. Bir ağda kullanılan donanım bileşenleri ve üzerinde çalışan veri iletim protokolleri ağın ne kadar fonksiyonel olduğunu gösterir. Yıllar içerisinde ağda

çalışan yazılım uygulamalarında gelişmişliğine bağlı olarak güvenlik çok boyutluluk kazanmıştır. Ayrıca ağda kullanılan her ürüne bağlı, farklı güvenlik modelleri kurgulanmalıdır. Bu modeller zaman içerisinde gelişen ve çeşitlenen standart güvenlik politikalarının yanı sıra kurumlara özel güvenlik politikaları ile de desteklenmelidir. Bilgi paylaşımı arttıkça, ağ ve bilgi güvenliği dün olduğundan daha fazla aranır olmuştur. Yanlış kullanımlar, kötü niyetli kullanıcılar, güvenli olmayan yazılımlardan dolayı hesap ve servislerin ele geçirilmesi, çalışanların zafiyeti gibi nedenlerden kaynaklanan tehditlerle mücadele etmek için bir güvenlik döngüsüne gereksinim vardır.

3. Ağ Güvenliği Yaşam Evreleri

İnternet yapısı ve karmaşıklığı itibarı ile güvensiz bir alandır. Kapalı yani internete bağlı olmayan ağlar günümüzde yok denecek kadar azdır. Bu demek oluyor ki siber suçlarla her an karşı karşıyayız. Birçok siber saldırı grubu dünya genelinde organize bir şekilde eylemler organize etmektedirler. Son günlerde adlarını Korsanlık Hareketi (hacktivizm) olarak duyuran bir gönüllüler grubu kendinden söz ettirmektedir. Bunlar iyi niyetli hacker'lerdir. Bir anda sosyal media üzerinden haberleşip seçilen bir kurban hedefe yoğun bir saldırı olayı gerçekleştirilmektedir. Genellikle hizmet engellemeye yönelik bu tip bir saldırılar dünya genelinde çok fazla ses getirmektedir. Genelde firmaların veya kurumların yürüttükleri faaliyetleri engelleme, bir takım belgeleri ve kritik bilgileri ele geçirme gibi toplu saldırılarla mağdurda imaj zedeleme yâda maddi kayıplar yaşatmaktadırlar. Bu ve benzeri siber saldırıların önlenebilmesi için standartlara dayalı bir güvenlik modeli uygulanmalıdır. Bunu bir politika planına dayalı olarak oluşturulan güvenlik ekseninde ele alınmalıdır. Uzun soluklu uygulanması gereken bu sürek ağ güvenliği ekseninde aşağıdaki şekil-1 de kurgulandığı gibi yaşamsal bir güvenlik döngüsü oluşturulmalıdır[3,10].



Şekil 1: Ağ güvenliği yaşam döngüsü

Bu yaşam döngüsü ile ağa yapılabilecek bir saldırıda olası güvenlik açıklıklarının oluşmasını önlemektir. Planlama, uygulama, kontrol etme ve önlem alma gibi temel süreçler takip edilerek sistemdeki zafiyetler tespit edilerek gerekli güçlendirmeler yapılır. Yama ve olay yönetimleri incelenip sıklıkla takip edilerek yeni güvenlik politika ve teknikleri ile yaşayan bir sistemin gelecekte de güncelliği korunacaktır[4].

3.1 Planlama

Bir ağın sağlıklı olarak güvenliğinin oluşturulması ancak o ağın özelliklerinin tam olarak tanınması ile mümkündür. Ağın tanınması demek kurulumundan işletimine kadar tüm mimarinin ve üzerinde yapılan tanımlamaların düzenli bir planlama ile kayıt altında tutulması ile mümkündür. Bu şekilde yapılan bir çalışmada iş sürekliliğinin sağlanmanın yanı sıra güvenlik politikalarının uygulanabilirliğini de kolaylaştırır. Örneğin ağınızın önünde istediğiniz kadar güvenlik duvarınız olursa olsun mimari yapı tam olarak bilinmeden bunların hiç bir önemi yoktur. Günümüz siber saldırıları çoğu güvenlik duvarı engellerini rahatlıkla geçebilmektedir. Çünkü saldırılar artık izin verilen standart hizmet portları üzerinden yapılmaktadır. Yani saldırgan sunucu havuzuna özellikle web kanalları üzerinden kolaylıkla ulaşabilmektedir. Dolayısıyla ağda var olan aktif cihazlar, IP aralıkları, yasaklı

ve izin verilen portlar, her türlü sunucu mimarisi ve aralarındaki veri iletişim hakları, kullanıcı ağı ve VLAN'ler arası geçiş tanımları gibi varlıklar ayrıntılı olarak yapılacak plana yansıtılmalıdır. Zaman içersinde yapılan her türlü yapılandırma değişiklikleri bu plan üzerine işlenerek güncelliği korunmalıdır. Sahada ve IT merkezinde görev alan çalışanlar sorumlu olduğu alanla ilgili belli seviyelerde ağ güvenlik eğitimlerine tabi tutulmalıdırlar.

3.2 Uygulama

Öncelikle kurumda kritik bilgi varlıklarının bulunduğu noktalar tespit edilir. Ağ mimari haritası üzerinde aktif cihazların konumu, sunucu yapılanması, kullanıcılar, varsa sanal ve özel ağ bölgeleri gibi var olan yapı tespit edilir. Kurum içi ve dışından bilgi varlıklarına erişim ihtiyacının tespiti, varsa hangi şifreli kanaldan hangi yetkilerle, kimlerin erişebileceği listesi hazırlanır. Ağ kullanıcılarının virüs koruması, kablolu-kablosuz erişim kimlik yönetimi, saldırı önleme sistemi, güvenlik duvarı gibi kurum için gerekli koruma düzeyleri ve sistem güvenlik gereksinimleri oluşturulur. Ağ güvenliği mimarisini oluştururken tek bir yöntem uygulanmamalıdır. Çünkü farklı yöntemler kullanılarak oluşturulan savunma engelleri, bir dizi güvenlik katmanının oluşmasına katkı sağlar. Bu katmanlar bir çeşit kurum içinde işlerin yürütülebilmesi için gerekli bilginin paylaşılması, dışarıya karşı ise korunmasını sağlar. Dahili ve harici her türlü ağ saldırılarına karşı önlem alınması özellikle internet üzerinden iş yapan kurumlar için bu bir zorunluluğa dönüşmüştür. Etkili bir güvenliğin uygulanması için tüm ağın izlenerek özellikle düğüm noktalarının veya ağ geçişlerinin yapıldığı aktif cihazlar üzerinde hak ve kısıtlamalar iyi tanımlanmalıdır. Sistemler üzerindeki ağ kullanıcıları doğru tanımlanmalıdır, bilgilere erişim yetkileri ortak kullanıcı adlarına değil bireysel şekilde açık ve belirleyici olmalıdır. Erişimin reddedilmesi veya kabul edilmesi kullanıcı kimliğine, yetki tanımlamasına, bağlantı zamanlamasına, geldiği ağ bağlantısının durumu gibi işle ilgili özel ölçütlere dayanabilir.

Uygulanacak güvenlik teknolojileri sistemi bilinen saldırılara karşı korumanın yanı sıra yeni saldırılara karşıda da aktif güncellenebilir yapıda olmalıdır. Ayrıca hızlı kurulabilir ve kurum personeli tarafından yetki ve tanımlamaların basitçe yapılabildiği kolay yönetilebilir yapıda olmalıdır.

3.3 Kontrol Etme

Güvenlik yapılanmasının testi ve olası açıklıklarının keşfedilmesi için daha önceden belirlenen sistem güvenlik haritası üzerinden yapılır. Kurum yöneticilerinin onayı alınarak oluşturulmuş ve tüm bölümlerde uygulanması gereken genel bilgi güvenliği politikaları ile erişim yetkileri, sınırlılıklar ve dışarıdan gelebilecek saldırılara karşı alınacak standart tedbirlerin neler olduğunun yazılı hale getirildiği doküman üzerinden takip edilir. Gerekli fiziksel yapılanma ve erişim bağlantıları göz yöntemi ile cihazlardaki yapılandırma tanımlamaların doğruluğu tanımlama yapanlar tarafından incelenerek test edilir. Daha sonra port açıklıkları ve siber ataklara karşı bazı güvenlik test yazılımları ile sistem saldırı dayanıklılık testine tabii tutulur. Ağın kapsamı ve üzerinde taşıdığı uygulamalara bağlı olarak bu tür test yazılımlarında bir veya birden fazla açık veya ticari yazılım uygulamalar kullanılabilir. Olası güvenlik açıklıkların tespit edilmesi halinde bunun türü, nedeni, hangi donanım veya yazılım üzerinde olduğu, açıklığın ne şekilde giderilebileceği hakkında durum raporu oluşturulur.

3.4 Önlem Alma

Tespit edilen bazı açıklıklar kritik seviyede olabilir ve kendi içinde risk puanlaması yapılarak hemen önlem alınması gerekir. Ağda iletilen bilginin maddi ve manevi değeri, başka ellere geçmesi durumunda ortaya çıkabilecek hasarın ölçüsü oranında

alınacak önlemin boyutu ve kaynak miktarı belirlenir. Güvenlik kontrolleri neticesinde tespit edilen bir açıklığın donanımsal ve yazılımsal boyutları ele alınır.

Donanımsal tarafta olan bir açıklık için öncelikle ağ haritası üzerinde yeri belirlenir. İlgili cihaz/cihazlar üzerinde çalışan yazılım güncellemeleri ve mevcut kural tanımlamaları kontrol edilir. Halen açıklık devam ediyorsa ek donanım veya üst düzel güvenlik desteğine sahip yeni donanım ürünü ile değiştirilmelidir. Bir ağda değiştirilmesi gereken çok sayıda cihaz olduğu bir yapı söz konusu olduğu durumda ilgili açıklığı önleyebilecek yeteneklere sahip bir güvenlik duvarı veya ağın bir kaç geçiş noktasına üst düzey layer 2,3 veya üstü cihazlarla trafik kontrol altına alınır. Bir ağ donanım cihazı üzerinden geçen veri paketlerinin türünü ne kadar çok tanıyabiliyorsa, içerik üzerinde güvenlik filtrelemesi daha kapsamlı hale getirilebilir.

Yazılım kaynaklı bir açıklık tespit edilmesi durumunda işletim sistemi veya uygulama yazılımı ön tespitleri yapılır. Bunun sunucu, istemci, geçerli tarayıcı veya ilgili kullanıcı tarafları sorgulanır. Her türlü yazılımlara ait anlık güncellemelerin ve yamaların takibi yapılır. Kurumdaki sunucu ve istemciler üzerinde mutlaka anti (virüs, trojan, malware..vb) zararlı yazılımlar ve içerik tarayıcılar aktif olmalıdır. Bu yazılımlar üzerinde gelen standart taramaların yanı sıra ilave ilgili kuruma özgü tanımlamalar ve kurallar yapılmalıdır. Kullanılmayan portlar ve hizmet servisleri mutlaka kapalı durumda olmalıdır[11].

Bir kuruma ait uygulanacak önlemin boyutu bilindik güvenlik açıklıklarının kapatılmasının yanı sıra o kuruma özgü bilgi varlıklarının nasıl ve ne şekilde tutulduğu, iletildiği, servis edildiği, bilgideki kritiklik düzeyi gibi pek çok değerler önlemin sınırlarını ve çeşitliliğini belirleyecektir. Bu oran, güvenlik kontrolü sırasında elde edilen risk tablosunun kritik seviyesine göre belirlenir. Tespit edilen güvenlik açıkları ve taşıdıkları riskler değerlendirilerek çözüm önerileri raporlanır. Bu işlemler uluslar arası güvenlik politikalarına dayalı olarak yapılmalıdır. Bilinen güvenlik önlemleri alınır. Önlem almada son aşama olarak sistemin üzerindeki bilgi varlıklarına yönelik "Penetrasyon Testi" denilen yöntemle en son dayanıklılık sızma testi gerçekleştirilir.

4. Ağ Güvenliği Dayanıklılık Testi

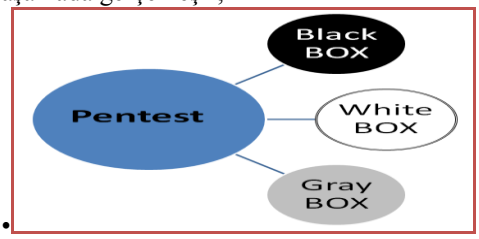
Ağ güvenliği test teknolojileri, bilişim sistemlerine yapılabilecek saldırıların önceden tespit edilmesine yönelik tarama ve raporlama işlemidir. Kişisel ve kurumsal gizli bilgilerinin ele geçirilmesi, kötüye kullanılması, virüs, spam, spyware, solucanlar gibi zararlı internet saldırı araçlarının verebileceği kötü sonuçları önlemek için ön tedbir niteliğindedir[7]. Ağ güvenlik testi yapılıp önlem alınmadığı durumlarda; yetkisiz erişimler, ağ ve çeşitli servislerin engellenmesi, hizmet kalitesinin düşürülmesi, uluslar arası güvenlik politikalarına uyumsuzluk ve bunun sonucunda tedbirsizlik nedeniyle yasal işlem riskleriyle karşı karşıya kalınabilir.

Şekil 2 – Zararlı yazılımlardaki artış oranı[12].

Şekil-2 de incelendiğinde 2011 yılının ikinci yarısından itibaren ortalama on aylık büyüme oranı% 60'dan fazla olmuştur. Bu artış oranı güvenlik alanında çok büyük riskleri beraberinde taşımaktadır. Zararlı yazılımlar ve sisteme sızmak isteyen saldırganların nelere sebep olabileceklerini önceden görülebilmek uluslar arası PCI, ISO27001, HIPAA gibi standartlar gereğidir[7]. Büyük ve kompleks bilişim altyapılarında güvenlik riski kaçınılmazıdır. Kuruluş kendi IT

çalışanlarının yanı sıra dışarıdan uzman üçüncü bir göz ile de güvenlik altyapısını test ettirmelidir. Bu tür testleri firma büyüklük ve risk düzeyine göre en az bir, ideal olanı ise iki defa yaptırılması yönündedir. Böylece ağ güvenliğinde süreklilik ve iyileştirmeler sağlanmış olur. Ağda kullanılan güvenlik cihazları da dahil, sanal ve bulut mimariler, mac, pc, notebook, tablet, ağ geçidi, her türlü ağ anahtarlama cihazlarının üzerindeki açıklıklar ve yama eksikliklerinin bulunması sızma testleri ile yapılır[2].

Sızma testleri Şekil-2'de görüldüğü gibi üç aşamada gerçekleşir;



Şekil-2 Sızma testi aşamaları

4.1 White Box (Beyaz Kutu Testi)

Güvenlik testine tabi olacak ağa ait IP aralıklar, ağ haritası, sunucular ve üzerinde çalışan servisler, bazı admin kullanıcı adı ve erişim şifrelerinin kullanılarak yapıldığı test biçimidir. Bu test daha çok iç ağ çalışanlarına ve işten ayrılan daha önce sistem yetkilerini üzerinde bulunduran kişilerin saldırı yapma senaryoları üzerine gerçekleşir.

4.2 Black Box (Siyah Kutu Testi)

Bu metod tamamen dışarıdan gelebilecek saldırılara karşı ağın dayanıklılık testine tabi tutulduğu bir çalışmadır. Çalışma yapacak kişilere önceden white test te olduğu gibi ağla ilgili herhangi bir bilgi verilmez. Zarar vermek amacıyla dışarıdan gelecek yabancı bir saldırgana karşı ağ bileşenlerinin içerideki bilgi varlıklarının güvenliğini ve dayanıklılığını test eder. Uzmanlık ve bilgiye dayalı emek-yoğun bir çalışma gerektirir.

4.3 Grey Box (Gri Kutu Testleri)

Ağ içerisinde normal statüde çalışan son kullanıcıların bilinçli veya bilinçsiz olarak sisteme verebilecekleri güvenlik zafiyetlerini test etmek için kullanılan yöntemdir. Yapılan araştırmalara kurum içi çalışanların ağ güvenliğine vermiş olduğu zarar dışarıdan gelen saldırı riskinden daha fazladır[3].

4. Sonuç ve Öneriler

Bildir de özetlenmeye çalışıldığı şekliyle bir bilgisayar ağına içeriden veya dışarıdan pek çok saldırı ile karşı karşıyayız. Önlem alınmamış ağ içerisinde dolaşan bir zararlı yazılım ile; sistemlere zarar vermek, bozulmalarını sağlamak, her tür bilgiyi karşı tarafa aktarmak, çalışan servisleri kesintiye uğratmak, bir cihaz veya sisteme giriş elde etmek ve saldırı atakları gibi tüm bu tür açıklıklara karşı penetrasyon testleri yapılarak, tespit edilen açıklıklar için derhal önlem alınmalıdır. Yapılan önlemler sonrasında yeniden doğrulama testleri yapılarak sonuçlar yönetimsel rapor haline getirilmelidir[10].

Güvenlik testleri ilgili firmanın talebi doğrultusunda gerçekleşir, aksi durumda hukuki siber saldırı durumu ortaya çıkar. Test öncesinde; test edilecek veya kapsam dışı bırakılacak bilgi varlıkları, gizlilik sözleşmesi ve tazminat metni gibi yasal süreçler karşılıklı imza altına alınmalıdır.

Tüm bu güvenlik test çalışmaları, sistemin büyüklüğüne göre 3-5 gün arasında süre gerektirebilir. Sızma ve dayanıklılık testlerini yapabilen opensource veya ticari bazı yazılımlar kullanılmaktadır. Bunlar; Backtrack, Nessus, Nmap, Hping, Metasploit, Canvas, Nexpose vb. Benzeri programlarla manuel veya otomatik tarama yöntemleri kullanılarak test işlemleri gerçekleştirilir[10]. Elde edilen tüm bilgi ve belgeler o kuruma ait belli gizlilik karinesi korunarak rapor haline getirilir. Bu test çalışmalarından elde edilen veriler ışığında bulunan güvenlik zafiyetleri ve sistem açıklıkları hemen kapatılır. Kapatıldıktan veya önlem alındıktan sonra

tekrar ilgili zafiyet yeniden kontrol testine tabi tutulur. Sistemin bütünü ile ilgili yapılacak güvenlik tarama test işlemleri ilgili işletmenin taşıdığı güvenlik riski ölçeğinde 6 ay-1 yıl gibi süre aralıklarında yenilenmesi gerekir.

Sonuç olarak günümüzde kurumlar bilgi güvenliği konusunda ciddi yatırımlar yapmaktadır. Bu yatırımların doğru ve güvenilir olması öncesinde ve sonrasında yapılacak dayanıklılık testleri ile mümkündür[9]. Görünen o ki bugün olduğu gibi gelecekte de güvenlik hep ön sıralarda yerini ve önemini koruyacaktır. Sistem içerisinde ağ güvenliğini sürekli yaşayan bir sistem olarak ele alınması gerekmektedir.

5. Kaynaklar

[1] Kevin Curran, Cyber Terrorism Attacks, Page: 1-6 pp. 2007

[2] www.eccouncil.org/CEH.htm

[3] http://en.wikipedia.org/

[4] www.cert.org/

[5] www.bilgiguvenligi.gov.tr

[6] Gary Hinson (IsecT Ltd, New Zealand) Information Security Awareness Page: 307-324 pp.

[7] E Şahinaslan, A Kantürk, Ö Şahinaslan, E Borandağ; Kurumlarda Bilgi Güvenliği Farkındalığı, Önemi ve Oluşturma Yöntemleri, Akademik Bilişim 2009, Şanlıurfa, S.1

[8] www.cisco.com/web/TR/security/

[9] http://www.computerworld.com.tr/

[10] http://seminer.linux.org.tr

[11] Ö Şahinaslan, E Şahinaslan M Razbonyalı, Open Source Administration Software and Implementation Results for ensuring Electronic Communication and Information Security Gediz University ISCSE 2010, Kuşadası, S.2

[12] http://www.symanteccloud.com/