Kurumsal Bilgi Güvenliği: Güncel Gelişmeler

Yılmaz VURAL, Şeref SAĞIROĞLU

***Özet*— Bilgi güvenliğindeki yeni gelişmelerin bilinmesi, güvenlikle ilgili yeni tehditlerin azaltılması ve kurumsal bilgi varlıklarının korunması açısından önemlidir. Kurumsal bilgi güvenliği yönetimi karmaşık süreçlere sahip olduğundan, bilgi güvenliği standartlarına uygun olarak yönetilmelidir. Kurumsal bilgi güvenliğinin yüksek seviyede sağlanması ile ilgili olarak literatürdeki mevcut kaynaklar araştırılıp incelendiğinde, kapsamlı ve güncel çalışmaların yetersiz olduğu, çoğunlukla ticari içerikli veya güvenilir olmayan web sitelerinde yer aldığı tespit edilmiştir. Bu araştırma çalışmasında kurumsal bilgi güvenliğiyle ilgili olarak son gelişmeler sunulmuştur.**

***Anahtar Kelimeler*— Anahtar Kelimeler Bilgi güvenliği, kurumsal bilgi güvenliği, bilişim güvenliği, bilgi güvenliği standartları, bilgi güvenliği yönetim sistemleri, web uygulama güvenliği, web tehditleri.**

***Abstract*— Being aware of new developments in information security is very important both for the protection of enterprise information assets and the reduction of risks which are related to new security threats. Since enterprise information security management has complex process, it should be managed in accordance within international security standards. When present information in the literature about maintaining Enterprise Information Security in high level is searched and examined, it is determined that comprehensive and current studies are not sufficient and mostly took part in the commercial web-sites or not reliable. In this paper, recent developments in the enterprise information security are presented.**

***Index Terms*— Information security, enterprise information security, IT security, information security standards, information security management systems, web application security, web threats.**

I. GIRIŞ

GÜNÜMÜZDE elektronik ortamlarda bilginin işlenmesi, taşınması ve saklanması kolaylaşmış, bilgiye mekândan bağımsız olarak istenilen ortamlardan erişilmesi sağlanmıştır. Günlük yaşantımızda yapmış olduğumuz birçok iş ve işlem ise kolaylıkla ve hızlıca yapılabilir hale gelmiştir. Elektronik ortamlarda kişiler ve kurumların sahip olduğu bilgilerin mahremiyetlerinin korunması, bu ortamların yaygınlaşmasının önünün açılması ve bu ortamlarda herhangi bir kaybın oluşmaması için bu ortamlarda bulunan bilgilerin güvenliğinin sağlanması gereklidir. Bilgi güvenliğini sağlamak toplumda sadece güvenlikle uğraşan kişi ve kuruluşların görevi değil bilgi çağı olarak adlandırılan günümüzde, bilgi sistemlerinin küreselleşmesi sonucunda bu sistemlerle herhangi bir şekilde doğrudan veya dolaylı yönden ilişkisi olan ve bu sistemleri kullanan tüm birey, kurum ve kuruluşların katkıda bulunması ve görev alması gereken önemli bir konu halini almıştır.

Yılmaz VURAL, STM A.Ş., Mecnun Sok. No:58 Beştepe, 06510 Ankara, yvural@stm.com.tr

Şeref SAĞIROĞLU, ,Gazi Üniversitesi MMF Bilgisayar Mühendisliği Bölümü, Maltepe, Ankara, ss@gazi.edu.tr

Kişilerin bilgi güvenliği önem arz ederken, bundan daha önemlisi, kişilerin güvenliğini doğrudan etkileyen kurumsal bilgi güvenliğidir. Bilgi güvenliği alanında yaşanan güvenlik ihlallerinin giderek artan bir bölümü ağ ve sistemlerden yazılımlara (uygulamalara) doğru kaymaktadır. Kurum bazında veya birey bazında güvenli ortamlarda iş yapma ihtiyaç ve istekleri her geçen gün hızla artmakta, kullanılan yazılımların güvenliği bilgi güvenliğinin sağlanmasında anahtar rol oynamaktadır [1,2]. Yıllar içerisinde ağ ve sistemlerin güvenliğinin sağlanmasına ilişkin geliştirilen yöntemler kurumlar tarafından başarıyla uygulanmış ve Sınır Ağ Güvenliği (Perimeter Network Security) kavramının önemi çoğu kuruluş tarafından anlaşılmış ve gerekleri yerine getirilmiştir. Ancak benzer durumu yazılım güvenliği için belirtmek zordur. Bilgi güvenliğinin sağlanmasında yazılım güvenliği merkezi ve kritik bir öneme sahiptir [3]. Günümüzde ağ ortamlarında çalışan kişiler ve diğer uygulamalar tarafından erişilebilen uygulama yazılımlarındaki güvenlik zafiyetleri kurumsal bilgi güvenliği tehditlerinin başında gelmektedir. Özellikle internet ortamında çalışan yazılımlara güvenlik göz ardı edilerek esneklik ve kullanım kolaylığı altında bir sürü eklentiler yapılması ise yangın halinde olan bir binaya benzin dökmekle eş anlamlıdır. Başlıca yazılım güvenliği tehditleri incelendiğinde çevresel değişkenler, bellek taşmaları, enjeksiyonlar, güvensiz ağ ve haberleşme ortamları, varsayılan sistem ayarları, programcı arka kapıları bilinmesi ve önlem alınması gereken önemli yazılım zafiyetlerdir.

Yazılımlardaki zafiyetlerin artarak güvenlik problemlerinin her geçen gün arttığı US-CERT (The United States Computer Emergency Readiness Team) koordinasyon merkezi tarafından yıllık olarak yayınlanan rapor ve istatistikî veriler incelendiğinde açıkça görülmektedir. US-CERT tarafından açıklanan güvenlik zafiyetleri 2004 yılında 3,780 iken, 2005 yılında 5,990'a ulaşmış 2006 yılında 8,064, 2007 yılının ilk altı ayında ise 3,907 olarak rapor edilmiştir [4].

Gartner ve Deloitte gibi bağımsız araştırma kuruluşlarının raporları incelendiğinde kurum ve kuruluşların güvenlik teknolojilerine yeterli ölçüde yatırım yapmadıkları görülmektedir. Deloitte firmasının 30 ülkede 2006 yılında gerçekleştirdiği araştırmada kurumların %73'nün güvenlik

yatırımı yaptığı, yatırım yapan firmaların bilgi işlem müdürlerinin %54'nün ise bu yatırımları yetersiz buldukları belirtilmiştir. Türkiye'de yapılan araştırmalarda ise 2005 yılı bilişim genel yatırımları 19 milyar dolar iken güvenlik yatırımları 30 milyon dolar, 2006 yılında bilişim yatırımları 23 milyar dolar iken güvenlik yatırımları 40 milyon dolara ulaşmakta ve 2007 yılında ise 47 milyon dolar olması beklenmektedir [5]. Bilgi güvenliğinin sağlanmasına yönelik kurumlar tarafından maddi yatırımlar yapılmadığında meydana gelen zararların ekonomik boyutu her geçen gün katlanarak artmaktadır. Bilgi güvenliği ihlallerinin meydana getirdiği zararlar yapılması gereken güvenlik yatırımlarıyla kıyaslandığında farkın çok büyük olduğu güvenlik firmalarının yapmış olduğu araştırmalar tarafından açıkça görülmektedir.

Kurumsal bilgi güvenliğinin yüksek seviyede sağlanmasında insan faktörü önemli bir yere sahiptir. İnsan faktörü sayesinde birçok güvenlik denetimi devre dışı bırakılabilmektedir. Yeterli düzeyde eğitim almamış kurum çalışanları (yönetici, teknik sorumlu, son kullanıcı) veya kurumsal bilgi sistemleri üzerinde yetkileri olan ve yerel saldırgan (internal hacker) olarak adlandırılan iyi niyetli olmayan üst derecede bilgiye sahip olan çalışanlar kurumsal bilgi güvenliğini üst düzeyde tehdit eden insan faktörleridir. Kurumsal bilgi güvenliği insan faktörü, teknoloji ve eğitim üçgeninde devamlılık gerektiren ve bu üç unsur arasında tamamlayıcılık olmadığı sürece yüksek seviyede bir güvenlikten bahsedebilmenin mümkün olamayacağı yönetilmesi zorunlu olan canlı bir süreçtir [6].

Günümüzde saldırganlar teknolojik olmayan ve engellenmesi daha zor olan sosyal yöntemleri sıklıkla tercih etmektedirler. İnsan faktörünü kullanarak bilgi güvenliği ihlalleri oluşmasını sağlayan aldatmaca sanatı teknik yöntemlere göre daha tehlikeli sonuçların oluşmasını sağlayan önemli ve güncel bir saldırı aracıdır [7]. Sosyal mühendis olarak adlandırılan aldatma sanatçılarının amaçları bilgiye erişim yetkisi olan kullanıcılar aracılığıyla güvenlik teknolojilerinin atlatılmasını (by-pass) sağlamaktır. Teknolojik önlemler sosyal mühendislik saldırılarından kurumları koruyamaz çünkü saldırganların hedefinde ne güvenlik duvarı, ne veri tabanı ne de bir web sunucusu vardır. Onlar için hedef sadece insanlardır [8]. Eğer hedef bir yazılım olsaydı yazılımın zafiyetini gidermek için yamalar yazılarak veya yeniden kodlanarak güvenli hale getirilebilirdi. Ancak söz konusu insan olduğundan güvenlik zafiyeti çalışanların bilgi güvenliği konusunda yeterli bilince ve bilgiye sahip olmasıyla giderilebilmektedir.

Önümüzdeki yıllarda dünyada ve ülkemizde bilgi güvenliği saldırılarının daha karmaşık yöntemlere dayanan ve etkilerinin çok daha geniş kitle ve ortamları tehdit edeceği gerçeği gözönüne alındığında, kurumsal bilgi güvenliğine yönelik güncel tehditleri anlatan, kurumları ve bireyleri bu tehditlere karşı bilinçlendirerek korunma yöntemlerini sunan güncel çalışmaların önemi daha iyi anlaşılacaktır.

II. KURUMSAL BILGI GÜVENLIĞI

Kurumsal bilgi varlıklarının güvenliği sağlanmadıkça, kişisel bilgilerin güvenliğide sağlanamaz. Bilgiye sürekli olarak erişilebilirliğin sağlandığı bir ortamda, bilginin göndericisinden alıcısına kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden bütünlüğünün sağlanması ve güvenli bir şekilde iletilmesi süreci bilgi güvenliği olarak tanımlanabilir [9]. Kurumsal bilgi güvenliği ise, kurumların bilgi varlıklarının tespit edilerek zafiyetlerinin belirlenmesi ve istenmeyen tehdit ve tehlikelerden korunması amacıyla gerekli güvenlik analizlerinin yapılarak önlemlerinin alınması olarak düşünülebilir

Kurumsal bilgi güvenliğinin sağlanmasının önemli gerekçeleri ana hatlarıyla aşağıda belirtilmektedir [10]. Bunlar;

-- Güvenlikle ilgili tehdit ve risklerin belirlenerek etkin bir risk yönetiminin sağlanması ve kurumsal itibarın korunması.

-- İş sürekliliğinin sağlanması.

-- Bilgi kaynaklarına erişimin denetlenmesi.

--Personelin, yüklenicilerin ve alt yüklenicilerin güvenlik konusunda bilinç düzeyinin yükseltilmesi ve önemli güvenlik konularında bilgilendirilmesi.

--Bilgi varlıklarının gizliliğinin, bütünlüğünün ve doğruluğunun sağlanması.

--Kurumsal bilgi varlıklarının kötü amaçlı olarak kullanma ve/veya suistimal edilmesinin engellenmesi,

--Bilgilerin güvenli bir şekilde üçüncü taraflara ve denetçilere açık olmasının sağlanması.

--Bilgi sistemlerini kullanan kişilerin, umursamazlığından, planlanmış taciz, bilinçsiz kullanım veya bilmeden yanlışlıkla suistimal etme gibi nedenlerden dolayı oluşabilecek donanım, yazılım ya da bilgisayar ağlarında meydana gelebilecek arızalara karşı korunması.

Bilgi güvenliğini sağlamak, planlamak, tasarlamak, gerçekleştirmek, işletmek, izlemek, denetlemek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçası Bilgi Güvenliği Yönetim Sistemi (BGYS) olarak tanımlanmaktadır [11]. Sadece teknik önlemlerle (güvenlik duvarları, atak tespit sistemleri, antivirüs yazılımları, anticasus yazılımlar, şifreleme, vb.) bilgi güvenliğinin sağlanması mümkün değildir. BGYS; insanları, süreçleri ve bilgi sistemlerini içine alan ve üst yönetim tarafından desteklenen bir yönetim sistemidir. Kurumlar açısından önemli bilgilerin ve bilgi sistemlerinin korunabilmesi, risklerin en aza indirilmesi ve sürekliliğinin sağlanması, BGYS'nin kurumlarda hayata geçirilmesiyle mümkün olmaktadır. BGYS'nin kurulmasıyla; olası risk ve tehditlerin tespit edilmesi, güvenlik politikalarının oluşturulması, denetimlerin ve uygulamaların kontrolü, uygun yöntemlerin geliştirilmesi, örgütsel yapılar kurulması ve yazılım/donanım fonksiyonlarının sağlanması gibi bir dizi denetimin birbirini tamamlayacak şekilde gerçekleştirilmesi anlamına gelmektedir.

Kurumsal bilgi güvenliği insan, eğitim, teknoloji gibi birçok faktörün etki ettiği yönetilmesi zorunlu olan karmaşık süreçlerden oluşmaktadır. Güvenlik sadece teknoloji problemi

olarak değil aynı zamanda insan ve yönetim problemi olarak değerlendirilmelidir [12]. Kurumlarda insan ve yönetim hatalarından kaynaklanan güvenlik ihlallerinin sebeplerine bakıldığında son kullanıcılardan üst yönetime kadar farklı kademelerde çalışan insanların ortak eksikliklerinin eğitim ve bilinçlendirme olduğu görülür. Kurumun stratejik hedeflerini belirleyen en üst seviyedeki yönetim kademelerinin kurumsal bilgi güvenliğinin sağlanması için verecekleri destek çok önemlidir. Bilgi güvenliğinin sağlanması için gerekli olan idari ve mali kararların verilebilmesi amacıyla yönetim tarafından bilgi güvenliği birimi kurulmalıdır. Bu birim tarafından güvenlikle ilgili stratejik kararlar zamanında ve doğru bir şekilde alınmalıdır. Yönetim tarafından bilgi güvenlik biriminin kurulması ve etkin bir yapıda çalışması yönetimin kurumsal bilgi güvenliğini sahiplendiğinin ve desteklediğinin önemli bir göstergesidir.

Kurumsal bilgi güvenliğinin üst seviyede sağlanmasına yönelik süreçlerinin oluşturulması, yönetilmesi ve yapılandırılması amacıyla yapılan standartlaşma çalışmaları dünyada ve ülkemizde hızla sürmektedir. Standartlaşma konusuna önderlik eden İngiltere tarafından geliştirilen BS–7799 standardı, ISO tarafından kabul görerek önce ISO–17799 sonrasında ise ISO–27001:2005 adıyla dünya genelinde bilgi güvenliği standardı olarak kabul edilmiştir [13]. Bilgi güvenliğiyle ilgili standartlar ilerleyen bölümlerde kapsamlı bir şekilde açıklanmıştır.

III. Kurumsal Bilgi Güvenliği Politikaları

Güvenlik politikaları kurum veya kuruluşlarda kabul edilebilir güvenlik seviyesinin tanımlanmasına yardım eden, tüm çalışanların ve ortak çalışma içerisinde bulunan diğer kurum ve kuruluşların uyması gereken kurallar bütünüdür [14]. Kurumsal bilgi güvenliği politikası, kurum ve kuruluşlarda bilgi güvenliğinin sağlanması için tüm bilgi güvenlik faaliyetlerini kapsayan ve yönlendiren talimatlar olup kurumsal bilgi kaynaklarına erişim yetkisi olan çalışanların uymaları gereken kuralları içeren resmi bir belge niteliğindedir.

Güvenlik politikaları kurumun üst düzey yönetimi tarafından desteklenmeli ve çalışanlar tarafından benimsenmelidir. Güvenlik politikası kullanıcılar tarafından uygulanabilir ve anlaşılabilir, güvenlik yöneticileri tarafından yönetilebilir olmalıdır. Bilgi güvenliği politikaları her kuruluş için farklılık gösterse de, genellikle çalışanın sorumluluklarını, güvenlik denetim araçlarını, amaç ve hedeflerini kurumsal bilgi varlıklarının yönetimini, korunmasını, dağıtımını ve önemli işlevlerin korunmasını düzenleyen kurallar ve uygulamaların açıklandığı genel ifadelerdir. Yönetimin, kurumsal bilgi güvenliği hakkında aldığı ayrıntılı kararları da içerir.

Politikalar içerisinde; gerekçelerin ve risklerin tanımlandığı, kapsadığı bilgi varlıkları ve politikadan sorumlu olan çalışanların ve gruplarının belirlendiği, uygulanması ve yapılması gereken kuralların, ihlal edildiğinde uygulanacak cezai yaptırımların, teknik terimlerin tanımlarının ve düzeltme tarihçesinin yer aldığı 7 bölümden oluşmalıdır [14]. Kurumsal Bilgi Güvenliği Politikası içerisinde bulunması gereken bölümler Çizelge 3.1'de gösterilmiştir.

Belli konularda çalışanların daha fazla bilgilendirilmesi, dikkat etmesi gereken hususlar, ilgili konunun detaylı bir şekilde ifade edilmesi istendiğinde alt politikalar geliştirilmelidir.

ÇİZELGE 3.1
Güvenlik Politikası Kısımları

Bölüm Adı	İçeriği
Genel Açıklama	Politikayla ilgili gerekçeler ve buna bağlı risklerin tanımlandığı kısım
Amaç	Politikanın yazılmasındaki amaç ve neden böyle bir politikaya ihtiyaç duyulduğu
Kapsam	Politikaya uyması gereken çalışan grupları (ilgili bir grup veya kurumun tamamı) ve hangi bilgi varlıklarını kapsandığını belirleyen kısımdır.
Politika	Uygulanması ve uyulması gereken kuralların yani politikanın yazıldığı kısımdır.
Cezai Yaptırımlar	Politika ihlallerinde uygulanacak cezai yaptırımların açıklandığı kısımdır
Tanımlar	Teknik terimlerin veya muğlâk ifadeler listelenerek açıklandığı kısımdır.
Düzeltme Tarihçesi	Politika içerisinde yapılan değişiklikler, tarihleri ve sebeplerinin yer aldığı kısımdır.

Örneğin kullanıcı hesaplarının oluşturulması ve yönetilmesi, şifre unutma, şifre değiştirme, yeni şifre tanımlama gibi durumlarda uyulacak kurallar alt politikalar aracılığıyla açıklanmalıdır. Bir diğer örnek ise, e-posta gönderme ve alma konusunda, üst yönetimin kararlarını, haklarını, kullanıcının uyması gereken kuralları alt politika içerisinde ifade etmek daha uygun olacaktır. Bu alt politikayla üst yönetimin, gerekli gördüğünde çalışanlarının e-postalarını okuyabileceği, e-postalar yoluyla gizlilik dereceli bilgilerin gönderilip alınamayacağı gibi hususlar, e-posta alt politikası içerisinde ifade edilebilir. Alt politikalar içerisinde, izin verilen yazılımlar, veritabanlarının nasıl korunacağı, bilgisayarlara uygulanacak erişim denetim ölçütleri, güvenlikle ilgili kullanılan yazılım ve donanımların nasıl kullanılacağı gibi konular da açıklanabilir.

Kurumsal bilgi güvenlik politikaları kuruluşların ihtiyaçları doğrultusunda temel güvenlik ilkelerinin (gizlilik, bütünlük ve erişilebilirlik) bazıları üzerinde yoğunlaşabilir. Örneğin askeri kurumlarda, bilgi güvenlik politikalarında genellikle gizlilik ve bütünlük ihlâlinin engellenmesi amaçlanmaktadır. Erişilebilirlik de önemlidir ancak birinci planda gizlilik ve

bütünlük gelmektedir. Askeri bir savaş uçağının kalkış zaman bilgilerinin onaylanıp yürürlüğe girmesi için düşmanlar tarafından görülmemesi (gizlilik) ve değiştirilmemesi (bütünlük) gereklidir. Bir diğer örnek ise kâr amacı gütmeyen işletmelerde uygulanan bilgi güvenlik politikalarında genellikle erişilebilirlik ve bütünlük ihlâlinin engellenmesi amaçlanmaktadır. Gizlilik unsuru da önemlidir ancak birinci planda erişilebilirlik ve bütünlük gelmektedir. Üniversite sınav sonuçlarının açıklandığı yükseköğretim kuruluşunda uygulanan güvenlik politikasında öğrenciler sınav açıklandıktan sonra istediği zaman diliminde (erişilebilirlik) doğru bir şekilde (bütünlük) sınav sonuçlarına bakabilmelidir.

İyi bir güvenlik politikası, kullanıcıların işini zorlaştırmamalı, kullanıcılar arasında tepkiye yol açmamalı, kullanıcılar tarafından uygulanabilir olmalıdır. Politika, kullanıcıların ve sistem yöneticilerinin eldeki imkânlarla uyabilecekleri ve uygulayabilecekleri yeterli düzeyde yaptırım gücüne sahip kurallardan oluşmalıdır. Alınan güvenlik önlemleri ve politikayı uygulayan yetkililer veya birimler yaptırımları uygulayabilecek idari ve teknik yetkilerle donatılmalıdır. Politika kapsamında herkesin sorumluluk ve yetkileri tanımlanarak kullanıcılar, sistem yöneticileri ve diğer kişilerin sisteme ilişkin sorumlulukları, yetkileri kuşku ve çelişkilere yer bırakmayacak biçimde açıkça tanımlanmalıdır. Politikalar içerisinde uygulanacak olan yasal ve ahlaki mahremiyet koşulları ile elektronik mesajların ve dosyaların içeriğine ulaşım, kullanıcı hareketlerinim kayıt edilmesi gibi denetim ve izlemeye yönelik işlemlerin hangi koşullarda yapılacağı ve bu işlemler yapılırken kullanıcının kişisel haklarının nasıl korunacağı açıklanmalıdır. Gerekli durumlarda istisnalar ve alternatif uygulamalar açıklanmalıdır.

Saldırıların ve diğer sorunların tespitinde kullanıcıların, yöneticilerin ve teknik personelin sorumluluk ve görevleri ile tespit edilen sorun ve saldırıların hangi kanallarla kimlere ne kadar zamanda rapor edileceği güvenlik politikalarında açıkça belirtilmelidir. Sistemlerin gün içi çalışma takvimleri, veri kaybı durumunda verinin geri getirilmesi koşulları gibi kullanıcının sisteme erişmesini sınırlayan durumlara politikalar içerisinde yer verilmelidir. Bu durumlarda kullanıcıya, izlemesi gereken yolu anlatacak ve yardımcı olacak kılavuzlara da yer verilmelidir.

IV. BILGI GÜVENLIĞI STANDARTLARI

Tehditlerin sürekli olarak yenilenmesi, kullanılan yazılım veya donanımlarda meydana gelen güvenlik açıklarının takibi, insan faktörünün kontrolü gibi süreçlerin takip edilebilmesi ve üst seviyede bilgi güvenliğinin sağlanması için bilgi güvenliği sürecinin yönetilmesi için bilgi güvenliği standartları kullanılmalıdır [15]. Bilgi güvenliğiyle ilgili standartlar takip eden alt bölümlerde açıklanmıştır.

A. İngiliz Standartları

BS–7799, bilgi varlıklarının gizlilik, doğruluk ve erişilebilirliğini güvence altına almak için uygulanması gereken güvenlik denetimlerini düzenleyen ve belgelendiren iki aşamalı İngiliz standartıdır. 1999 yılında yayınlanan ilk sürümün birinci bölümünde bilişim güvenliği için çalışma kuralları anlatılmakta olup (Information Technology–Code of Practice for Information Security Management) 10 bölüm içerisinde 36 kontrol 127 alt kontrol maddesi bulundurmaktadır. İkinci bölümde (Information Security Management Systems–Specification with Guidance for Use) bilgi güvenliği yönetim sistemini planlamak, kurmak ve devam ettirmek için gerekli olan süreçler adım adım tanımlamakta ve bilgi güvenliği yönetim sistemine ait belgelendirme (sertifikasyon) bu kısımda yapılmaktadır.

BS–7799 kurumların sadece kendi bilgi güvenlik prosedürlerini değil birlikte çalıştıkları iş ortaklarıyla ilgili sözleşmelerinde bilgi güvenliği yönünden analiz edilmesine yardımcı olmaktadır. Standardın tarihsel oluşumuna bakıldığında 1993 yılında Kural rehberi, 1995 yılında İngiliz standardı, 1998 yılında Sertifikasyon tarifi yapılmış 1999 yılında büyük bir düzeltmeden geçerek birinci kısmı, 2002 yılında ise ikinci kısmı yayınlanmıştır [16].

Bilgi güvenliği yönetim sistemleriyle ilgili diğer bir İngiliz standardı Aralık 2005'te BS7799–3:2005 Bilgi Güvenliği Yönetim Sistemleri Risk Yönetiminin Kuralları ismiyle hazırlanmıştır. Standart 2006 yılında tekrar gözden geçirilmiş ve BS7799–3:2006 ismiyle yayınlanmıştır. BS7799–3 standardı BS7799–2 standardının uygulanması için destek sağlayarak ölçeklenebilir (küçük, orta veya büyük kurumlar) yapıda standardın yaygınlaşmasına yardımcı olması için geliştirilmiştir. Standard içerisinde risk değerlendirmesi, belirlenen risklere kontrollerin uygulanması, tanımlanmış risklerin izlenmesi, kontrol yönetim sistemlerinin bakımı gibi risk yönetimi ile ilgili konular üzerine odaklanılmıştır. Kapsamın belirlenmesi, kural oluşturan referanslar, terimlerin tanımı, kurum bağlamında risk, risk değerlendirmesi, risk kararının verilmesi, risk yönetimi BS7799–3 standardının bölümlerini oluşturmaktadır [17].

B. ISO/IEC Standartları

Uluslararası Elektroteknik Komisyonunu (The International Electrotechnical Organization-IEC) 1906 yılında Uluslararası Standartlar Organizasyonu (International Organization for Standardization-ISO) 1947 yılında uluslararası alanda ticari (ISO) ve elektroteknik (IEC) standardizasyonun sağlanması için, İsviçrenin Cenova şehrinde kurulmuştur [18]. ISO ve IEC birlikte teknik çalışma grupları oluşturarak (Joint Technical Committee-JTC) tüm dünyada geçerli olacak standartlar oluşturmaktadırlar. Bununla birlikte ISO tarafından IT Güvenlik Standartları ile ilgili çalışmalar JTC–1 Bilişim Teknolojileri Komitesine bağlı SC 27: BT Güvenlik Teknikleri Alt Komisyonunda ele alınmaktadır. Bilgi güvenliği konusunda çalışan bu komisyonun sorumluluklarından bazıları aşağıda belirtilmiştir [19].

--Bilgi teknolojileri sistemleri güvenlik hizmetlerinin ve ihtiyaçların tanımlanması.

--Güvenlik teknikleri ve mekanizmalarının geliştirilmesi.

-- Güvenlik kılavuzlarının geliştirilmesi.

--Yönetim destek dokümanları ve standartların geliştirilmesi.

Yukarıda açıklanan görevleri yerine getirmek üzere bu komisyon içinde 5 ayrı çalışma grubu (Working Group) bulunmaktadır. Bu gruplar aşağıda belirtilmiştir.

--Çalışma Grubu–1 (JTC 1/SC 27/WG 1): Bilgi güvenliği yönetim sistemleri.

--Çalışma Grubu–2 (JTC 1/SC 27/WG 2): Şifreleme ve güvenlik mekanizmaları

--Çalışma Grubu–3 (JTC 1/SC 27/WG 3): Güvenlik değerlendirme kriterleri.

-- Çalışma Grubu–4 (JTC 1/SC 27/WG 4): Güvenlik denetimleri ve hizmetleri.

-- Çalışma Grubu–5 (JTC 1/SC 27/WG 5): Kimlik yönetimi ve mahremiyet.

SC27'ye bağlı çalışma gruplarından Çalışma Grubu–1 (WG1), bilgi güvenliği yönetim sistemleri standartları (ISO/IEC 17799, ISO/IEC 27000 Serisi) ile ilgili çalışmaları yürütmektedir.

ISO/IEC 17799 standardı: BS–7799 standardının ikinci sürümü Mayıs 1999'da çıktığında ISO BSI'nın yayınladığı çalışmayla ilgilenmeye başlamıştır. Aralık 2000'de, ISO BS–7799 standardının ilk bölümünü alarak ISO/IEC 17779 olarak yeniden adlandırmış ve yeni bir standart olarak yayınlamıştır. ISO 2005 yılında bir düzenlemeye giderek 27000 serisini bilgi güvenliğiyle ilgili standartlara ayırmıştır [20].

ISO/IEC 27000-27059 arasındaki standartlar ISO tarafından SC27 grubu tarafından çalışılan bilgi güvenliğiyle ilgili standartlara ayrılmıştır. Çizelge 4.1'de gösterilen standartların hepsi yayınlanarak kullanıma açılmamıştır. Yayınlanan standartlara ek olarak geliştirme ve düşünce aşamasında olan standartlara ait kısa açıklamalar aşağıda verilmiştir [21].

ISO/IEC 27000, serisinde yer alan standartlar içerisinde geçen teknik terimler ve açıklamalarının yer aldığı genel bir sözlük formatında geliştirilmektedir.

ISO/IEC 27001, BGYS için gereklilikleri ortaya koyan bir standarttır. Bilgilerin düzenli olarak maruz kaldığı tehditlerin tanımlanmasına, yönetilmesine ve bunların minimize edilmesine yardımcı olur. BGYS kurmak, gerçekleştirmek, işletmek, izlemek, sürdürmek ve iyileştirmek için ISO/IEC 17799:2005 standartındaki kontrollerin uygulandığı süreçleri tanımlar.

BS–7799 standartının ikinci bölümü üzerinde bazı iyileştirmeler ve değişiklikler yapılarak ISO/IEC Çalışma Grubu–1 tarafından 15 Ekim 2005 tarihinde standart olarak yayınlanmıştır. Bu standardın yayınlanmasından sonra İngiliz BS7799–2 standartı iptal edilmiş ve yerini ISO/IEC 27001 standartıyla içeriği aynı olan BS-ISO/IEC 27001 standardı almıştır. Bu standart kurumların büyüklüğüne bakılmaksızın BGYS kurulması bakım ve idamesi ile ilgili kurumlara yardım etme ve belgelendirme amacıyla oluşturulmuştur. ISO/IEC 27001 standardı yönetim standartlarıyla (ISO 9001, ISO 14001) uyumlu olarak geliştirildiğinden yönetim standartlarının gereklerinide yerine getirmektedir.

ISO/IEC 27002, halen hazırlanma aşamasındadır. Bu standardın daha önceki bölümde açıklanan ISO/IEC

ÇİZELGE 4.1
ISO 27000 SERISI STANDARTLARI

Standart Adı	Açıklaması
ISO/IEC 27000–27059	Bilgi güvenliğiyle ilgili standartlar için ayrılmış aralık
ISO/IEC 27000	BGYS standartları için genel bir sözlük (hazırlanıyor)
ISO/IEC 27001	BGYS ihtiyaçları (BS7799 Bölüm–2) (2005 yılında yayınlanmıştır)
ISO/IEC 27002	BGYS uygulama ilkeleri (ISO/IEC 17799:2005)
ISO/IEC 27003	BGYS uygulama rehberi (hazırlanıyor)
ISO/IEC 27004	BGYS metrikleri ve ölçüm (hazırlanıyor)
ISO/IEC 27005	BGYS risk yönetimi (hazırlanıyor)
ISO/IEC 27006	BGYS belge kaydı ve belgelendirme süreçleri kılavuzu (hazırlanıyor)
ISO/IEC 27007	BGYS izleme (Audit) için kılavuz (hazırlanıyor)
ISO/IEC 27031	ISO/IEC 17799/27002 standardının Telekom sektörü için uyarlanması (hazırlanıyor)

17799:2005 standardına eşdeğer olması beklenmektedir. Bilgi güvenliği ile ilgili standartların 27000 serisi altında yer almasından dolayı ISO/IEC tarafından öyle bir düzenlemeye gidilmiştir. Tahmini olarak 2007 yılı sonlarında yayınlanması beklenmektedir.

ISO/IEC 27003, 27001 standardının nasıl kullanılacağına dair açıklamalar ve örnekler içeren uygulama rehberi olarak geliştirilmekte olup tahmini olarak 2008 yılının ekim ayında standart olarak yayınlanması beklenmektedir.

ISO/IEC 27004, halen geliştirilme aşamasında olan bu standart bilgi güvenliği yönetim metrikleri ve ölçümüne tahsis edilmiştir. Bilgi güvenliği yönetim sistemlerinin etkinliğinin ölçülmesi ve raporlanmasında kurumlara yardımcı olması beklenen bu standardın tahmini olarak 2007 yılsonu veya 2008 başlarında yayınlanması beklenmektedir.

ISO/IEC 27005, halen geliştirilme aşamasında olan bu standart BS 7799 Kısım–3 "BS 7799–3:2006 – Bilgi Güvenliği Yönetim Sistemleri – Bilgi Güvenliği Risk Yönetimi Kılavuzları" isimli İngiliz standardının ISO tarafından uyarlanması çalışmasını içermektedir. 2008 veya

2009 yılı içerisinde yayınlanması tahmin edilmektedir. BS 7799–3:2006 standardı 16 Mart 2006 tarihinde İngiliz standardı olarak kabul edilmiş, risklerin değerlendirilmesi, kontrollerin uygulanması, risklerin düzenli olarak izlenmesi ve gözden geçirilmesi gibi konu başlıklarını içermektedir.

ISO/IEC 27006, halen geliştirilme aşamasında olan bu standart "Bilgi Teknolojileri Felaket Önleme Hizmetleri Kılavuzu" ismiyle duyurulmuş ve tahmini olarak Kasım 2007 yılında yayınlanması planlanmaktadır.

ISO/IEC 27007, ISO 27001 standartına göre BGYS denetlemesinde kullanılacak kılavuz niteliğinde geliştirilmesi düşünülen bu standart 2009 yılında tamamlanması beklenmektedir.

ISO/IEC 27031, standardı ISO 17799/27002 standartı esas alınarak Telekom sektörü için geliştirilmektedir. 2007 yılı ortalarında ITU-T X.1051 ve ISO/IEC 27031 ismiyle yayınlanması beklenmektedir.

C. Türkiyede Bilgi Güvenliği Standartları

Türkiye'de bilgi güvenliği standartlarıyla ilgili çalışmalar ve belgelendirmeler, Türk Standartları Enstitüsü (TSE) tarafından yapılmaktadır. TSE teknik kurulunun ISO/IEC 17799:2000 standardını tercüme ederek 11 Kasım 2002 tarihinde aldığı karar ile TS ISO/IEC 17799 Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri Türk standardı olarak kabul edilmiştir. TS ISO/IEC 17799 standardı, kuruluşlar bünyesinde bilgi güvenliğini başlatan, gerçekleştiren ve sürekliliğini sağlamak için, bilgi güvenlik yönetimi ile ilgili tavsiyeleri içeren belgelerdir.

BGYS belgelendirilmesine yönelik TSE teknik kurulu tarafından yapılan çalışmalar sonucunda BS 7799–2:2002 standardının tercümesi yapılarak "Bilgi güvenliği yönetim sistemleri–Özellikler ve kullanım kılavuzu" ismiyle TS 17799–2 standardı olarak 17 Şubat 2005 tarihinde kabul edilmiş ve yürürlüğe girmiştir. Ancak TS ISO/IEC 27001:2006 "Bilgi teknolojisi–Güvenlik teknikleri-Bilgi güvenliği yönetim sistemleri–Gereksinimler", 2.3.2006 tarihinde Türk standartı olarak kabul edildiğinden TS 17799–2 standartı TSE tarafından iptal edilmiştir [22].

TS ISO/IEC 27001:2006 standardı, tüm kuruluş türlerini (örneğin, ticari kuruluşlar, kamu kurumları, kâr amaçlı olmayan kuruluşlar) kapsar. Bu standart, bir BGYS'yi kuruluşun tüm ticari riskleri bağlamında kurmak, gerçekleştirmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için gereksinimleri kapsar. Bağımsız kuruluşların ya da tarafların ihtiyaçlarına göre özelleştirilmiş güvenlik kontrollerinin gerçekleştirilmesi için gereksinimleri belirtir. Bu standart ISO/IEC 27001:2005 standardından yararlanarak hazırlanmıştır. ISO/IEC 27001:2005 standardının tercümesidir.

D. Genel Bir Değerlendirme

Kurum veya kuruluşların üst düzeyde bilgi güvenliğini ve iş sürekliliğini sağlamaları için, teknik önlemlerin yanında teknik olmayan (insan faktörü, prosedürel faktörler, vb.) önlemlerin ve denetimlerin alınması, tüm bu süreçlerin devamlılığının sağlanılması ve bilgi güvenliği standartlarına uygun olarak yönetilebilmesi amacıyla yönetim tarafından desteklenen insanları, iş süreçlerini ve bilişim teknolojilerini kapsayan bilgi güvenliği standartlarına uygun olarak BGYS kurmaları gerekmektedir. Bilgi güvenliği standartları kurumların kendi iş süreçlerini bilgi güvenliğine yönelik risklerden korumaları ve önleyici tedbirleri sistematik biçimde işletebilmeleri ve standartların gereğini yerine getiren kurum veya kuruluşların belgelendirilmesi amacıyla geliştirilmiştir.

Ülkemizde genellikle güvenlik politikaları standartlara uygun olmadan yazılı veya sözlü, onaylı veya onaysız bir biçimde kuruluşlar tarafından uygulanmakta ve çoğu kurum tarafından da bilgi güvenliği yönetimi için yeterli görülmektedir. Bu yanlış anlamanın giderilmesi için dünya genelinde kabul görmüş ve uygulanabilirliği test edilmiş bilgi güvenliği standartları esas alınarak kuruluşların bilgi güvenliği yönetimi konusunda eksikliklerini gidererek BGYS kurmaları ve belgelendirilmeleri gerekmektedir. BGYS çerçevesinde oluşturulacak güvenlik politikalarına üst yönetim ve tüm çalışanların destek vermesi ve tavizsiz bir şekilde uygulanması, işbirliğinde bulunulan tüm kişi ve kuruluşlarında bu politikalara uyma zorunluluğu, kurumsal bilgi güvenliğinin üst düzeyde sağlanmasında önemli bir faktördür.

BGYS standartlarının kurumlara uyarlanması, anlatılması, kullanıcı, teknik çalışanların ve yöneticilerin eğitilmesi konusunda kuruluşların danışmanlık hizmetleri almaları gerekmektedir. BGYS uygulamaları kurumlar tarafından başarılı bir şekilde uygulandıktan sonra kuruluşların bilgi güvenliğini yönettiklerine dair uluslararası alanda geçerli olan belgeler alması bilgi güvenliğinin kritik olduğu kurumlar açısından önemli bir göstergedir.

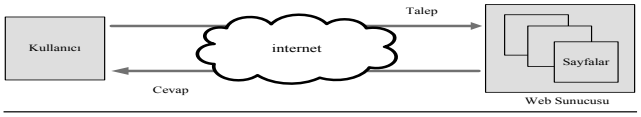
V. KURUMSAL BILGI GÜVENLIĞINDE GÜNCEL TEHDITLER

Kurum ve kuruluşlar bilgilerini elektronik ortamlara açtıkça, elektronik ortamlarda yapılan iş ve işlemler artmakta karşılaşılan tehdit ve tehlikelerde de doğal olarak artışlar gözlenmektedir. Son yıllarda yapılan araştırmalar ve çalışmalar incelendiğinde kurumsal bilgi güvenliğinin üst seviyede tehdit eden ve korunmasızlık seviyesinin en yüksek olduğu güncel tehditleri içeren ortam olan web uygulamaları bu bölümde ele alınmıştır [23, 24, 25].

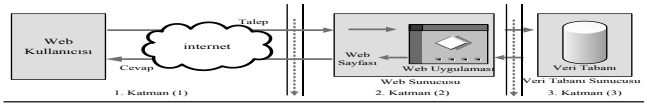
Web uygulamaları, güncel bilgiye kurum, kuruluş veya bireylerin kolayca erişebilmesi için en kolay ve en etkin yöntem olarak karşımıza çıkmaktadır. Web denilince akla ilk olarak kurumların vitrini ve itibarı haline gelmiş kurumsal web siteleri gelmektedir. Web üzerinden verilen hizmetler çoğaldıkça web'e yönelik tehditler ve saldırılar da artışlar gözlemlenmektedir. Bunun nedeni, web uygulamaları güvenliğinin ilgisizlikten ve bilgisizlikten kaynaklanan sebeplerden ötürü yeterince ciddiye alınmaması ve güvenli yazılım geliştirme tekniklerinin bilinmemesi veya kullanılmaması olarak açıklanabilir.

Web sitelerinin çalışma prensipleri güncel web tehditlerinin daha iyi anlaşılabilmesi amacıyla kısaca aşağıda açıklanmıştır. Web uygulamalarının üzerinde çalıştığı Web siteleri Şekil

5.1'de şematik olarak gösterildiği gibi dinamik veya statik yapıda çalışan içerikler sunmaktadırlar. Şekil 5.1 (a)'da gösterilen ve statik yapıda çalışan web siteleri, kullanıcıdan gelen talepler üzerine ilgili web sayfalarının gösterilmesini sağlayan statik HTML kodlarını içermektedirler.



(a) Statik



(b) Dinamik

Şekil 5.1. Web sitelerine ait çalışma yapılarının şematik gösterimi

Statik web siteleri günümüzde yerlerini artık dinamik içerikli web sitelerine veya portallarına bırakmaktadır. Dinamik web siteleri, kullanıcı istekleri doğrultusunda çalışan web uygulamaları içermektedir. Dinamik web siteleri Şekil 5.1 (b)'de şematik olarak gösterildiği gibi üç katmanlı bir yapı içerisinde çalışmaktadır [26].

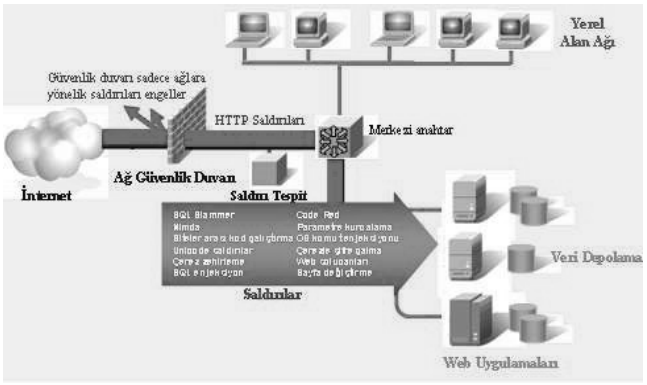
Şekil 5.1 (b) 'de gösterilen katmanlar aşağıda maddeler halinde kısaca açıklanmıştır.

(1) Web siteleri için taleplerin başladığı Web tarayıcılarıdır (Internet Explorer, Mozilla, Firefox, Netscape, vb.). Web tarayıcıları üzerinden kullanıcılar, web sunucusuna içerikle ilgili taleplerini iletirler.

(2) Dinamik sayfaların üretildiği uygulama katmanıdır (Hypertext Processor-PHP, Active Server Pages-ASP, Java Server Pages-JSP, WebSphere, ColdFusion, SunONE, vb.).

(3) Web uygulamaları tarafından kullanılan verilerin depolandığı veri tabanlarıdır (MS SQL, My SQL, Informix, Oracle, vb.).

Dinamik içerikli web sitelerinde, web tarayıcıları taleplerini web uygulamalarına ilettikten sonra bu istekler doğrultusunda veritabanı sorgulaması yapılır ve talep edilen isteklere ait sonuçların yer aldığı sayfalar üretilerek, tarayıcılar üzerinde gösterilir. Dinamik içerikli web sayfaların bu esnek çalışma yapısı birçok güvenlik tehdidini ve ihlâllerini beraberinde getirmektedir. Gartner Grup tarafından yapılan bir araştırmada bu durum açıkça ortaya konmaktadır. Günümüzde yapılan saldırıların %70'i uygulama seviyesindeki ataklardan kaynaklanmakta ve ticari içerikli web sitelerin %75'i ise korunmasız durumdadır [27]. Web uygulamalarında oluşabilecek bir zafiyet, güvenlik önlemlerini (güvenlik duvarı, saldırı tespit ve önleme sistemleri, vb.) Şekil 5.2'de gösterildiği gibi devre dışı bırakarak güvenilir bölgede yer alan sistemleri üst düzeyde tehdit etmektedir.



Şekil 5.2. Güncel web tehditleri

Web uygulamalarının güvenliğiyle ilgili birçok çalışma yapılmaktadır. Bu çalışmalardan birisi olan, Mark Curphey tarafından 2001 yılında kurulan, kâr amacı güdmeyen ve herkese açık bir ortam olan OWASP (The Open Web Application Security Project) web uygulama güvenliğinin artırılmasına yönelik ücretsiz araçlar, standartlar, web uygulamaları güvenliğiyle ilgili forumların yapılması, makalelerin yazılması konusunda çalışmaktadır [28]. Diğer bir çalışma ise 2004 yılında Jeremiah Grossman ve Robert Auger tarafından kurulan ve web uygulamaları güvenliğiyle ilgili açık standartların geliştirilmesi, yaygınlaştırılması ve kullanımı gibi konularda çalışan Web Uygulamaları Güvenlik Konsorsiyumudur (The Web Application Security Consortium-WASC) [29].

Kurumsal Bilgi Güvenliğini üst seviyede etkileyen güncel tehditler takip eden alt başlıklarda kısaca açıklanmıştır.

A. Kimlik Doğrulama Tehditleri

Web uygulamalarında yer alan kimlik doğrulama mekanizmasını atlatmak veya istismar etmek için kullanılabilecek zafiyetlerin oluşturduğu tehditlerdir. Kimlik doğrulamasında "sahip olunan bir nesne", "bilinen bir bilgi" veya "sahip olunan bir özellik" kullanılmaktadır [30]. Kimlik doğrulama saldırıları, web sitesinin kullanıcı, servis veya uygulama kimliğini doğrulayan sistemleri hedef alan tehditleri kapsar.

B. Yetkisiz Erişim Tehditleri

Yetkilendirme saldırıları, bir web uygulamasının kullanıcı, servis veya uygulamanın istenen bir işlemi gerçekleştirmesi için gereken izinleri belirlemek için kullanılan yöntemleri hedef almaktadır. Yetkilendirme tehditlerini, oturum bilgisi tahmin etme, yetersiz yetkilendirme, yetersiz oturum sonlandırma, oturum sabitleme olmak üzere kendi arasında dört grupta sınıflandırmak mümkündür. Yetki veya oturum bilgisi tahmin etme, web uygulamasının kullanıcısı rolüne girme veya söz konusu kullanıcının oturumunun ele geçirilmesi yöntemidir. Yetersiz yetkilendirme, web uygulamalarının daha geniş erişim kontrol kısıtlamaları gereken hassas bilgiye, yapılandırma hatalarından kaynaklanan zayıflıklardan faydalanılarak erişme yöntemidir. Yetersiz oturum sonlandırma, web uygulamlarının yetkilendirme için

kullanılan eski oturum kimlik bilgisini tekrar kullanma imkanı vermesinden kaynaklanmaktadır. Oturum sabitleme, daha önceden belirlenen bir oturum numarasının çeşitli yöntemlerle kullanıcılara tahsis ettirilmesini sağlamaktadır [31, 32, 33].

C. Kullanıcı Taraflı Tehdtiler

Kullanıcı taraflı tehditler, web sitesi ve kullanıcı arasında kurulan güvenin istismar edilmesi üzerine odaklanır. Yasal olan web siteleriyle, kullanıcıları arasında teknolojik ve psikolojik bir güven kurulmaktadır. Kullanıcı, web uygulamalarının geçerli içerik sunmasını beklerken web uygulamasından herhangi bir saldırı gelmesini beklemez. İçerik sahteciliği (Content Spoofing) ve siteler arası kod çalıştırma (Cross Site Script-XSS) kurumsal bilgi güvenliğini etkileyen kullanıcı taraflı tehditlerdir. İçerik sahteciliği, kullanıcının ziyaret ettiği dinamik içerikli web sitesinde harici olarak çalışan web uygulamasının ziyaret edilen web sitesinin resmi içeriği olduğuna inandırılmasını sağlayan saldırı yöntemidir. Bu yöntem kullanıcı ile web sitesi arasındaki güveni istismar ederek giriş formları, tahrif edilmiş içerik ve yanlış yayın sürüm bilgileri içeren sahte web siteleri oluşturmak için kullanılmaktadır. Siteler arası kod yazma, kullanıcı ile web sitesi arasındaki güven ilişkisi istismar edilerek, web sitesinin saldırgan tarafından belirlenen çalıştırılabilir kodu kullanıcıya göndermesi ve bu kodun kullanıcı web tarayıcısında yüklenerek çalışmasıyla gerçekleşmektedir [34, 35, 36].

D. Komut Çalıştırma

Komut çalıştırma, web uygulamalarında uzaktan çalıştırılan komutlar yardımıyla yapılan tehditlerdir. Web uygulamaları HTTP üzerinden gelen istekler (kullanıcı girdileri) doğrultusunda nasıl davranacağına karar vermektedir. Çoğu zaman bu kullanıcı girdileri dinamik web sitesi içeriğinin hazırlanılmasında kullanılan komutların çalıştırılmasını sağlarlar. Eğer dinamik web sitelerinin içeriğinin hazırlanmasında kullanılan bu komutların kodlanmasında güvenlik ölçütleri göz önüne alınmaz ve girdi doğruluğu sınanmazsa, çalıştırılan komutların saldırganlar tarafından manipüle edilmesi sonucu web siteleri üzerinde güvenlik ihlalleri oluşur.

E. Bilgi Açığa Çıkarma

Bilgi açığa çıkarma, web uygulamalarının kendisi veya çalıştığı platformlarla ilgili sisteme özel (versiyon, çalıştığı platform, yama seviyesi, yedek veya geçici dosyaların yeri, vb.) bilgilerin elde edilmesi için yapılacak işlemleri kapsamaktadır. Çoğu durumda, web uygulamaları kendileri hakkında bir kısım bilgiyi gösterecektir. Ancak burada önemli olan mümkün olduğunca, uygulamalar hakkında gösterilen bilgilerin boyutu en aza indirgenmektedir. Uygulamalar ve çalıştığı platformlar hakkında ne kadar çok bilgi toplanırsa saldırganlar tarafından zafiyetlerin belirlenmesi ve kullanılmasıda o kadar kolay olur.

F. Genel Değerlendirme

Güncel tehditler ve çalışmalar incelendiğinde kurumsal bilgi güvenliği tehditlerininin ağ ve sistemlerden web uygulamalarına doğru hızlı bir şekilde kaymakta olduğu görülmektedir. Dünyada olduğu ve literatürde de vurgulandığı gibi ülkemizde en fazla güvenlik açığına web uygulamalarında rastlanmaktadır. Kurumların genelde sınır ağ güvenliğinin (Perimeter Network Security) sağlanmasıyla ilgili çözümleri (güvenlik duvarı, saldırı tespit sistemleri, antivirüs programları, vb.) ve farkındalıkları olduğu saptanmıştır. Ancak web uygulama güvenliği kavramının dünyada olduğu gibi ülkemizde de, uygulamayı geliştiren yazılımcılarında dahil olduğu büyük bir çoğunluk tarafından anlaşılamadığı, bilinmediği veya bilinse dahi uygulanamadığı görülmektedir.

Kurum veya kuruluşların üst düzeyde bilgi güvenliğini ve iş sürekliliğini sağlamaları için standartlar çerçevesinde teknik önlemlerin uygulanmasının yanında teknik olmayan (insan faktörü, prosedürel faktörler, vb.) önlemlerin ve denetimlerin alınması, tüm bu süreçlerin devamlılığının sağlanılması ve bilgi güvenliği standartlarına uygun olarak yönetilebilmesi amacıyla yönetim tarafından desteklenen insanları, iş süreçlerini ve bilişim teknolojilerini kapsayan bilgi güvenliği standartlarına uygun olarak BGYS kurmaları gerekmektedir.

VI. SONUÇ

Elektronik ortamlar ülkemizde her geçen gün hızla yaygınlaşmakta, ticari ve günlük yaşantımızdaki varlığını hissedilir oranda arttırmaktadır. Elektronik ortamın doğasında var olan güvensizlik unsuru, elektronik ortamlardaki uygulamaları tehdit eden en büyük unsurdur. Geçmiş yıllarda saldırılar, yaygın ve hedef gözetmeksizin yapılmaktayken artık nokta hedefi gözeten ve bölgesel olarak düzenlenen saldırılar yapılmaktadır. E-posta ve anlık mesajlaşma yoluyla gelen tehditlerin yanı sıra, web'in kendisi de ciddi bir tehdit unsuru haline gelmiştir. Günümüzde e-posta ve web tehditlerinin birleşmesiyle çok zararlı ve bulaşıcı virüsler doğmaktadır. Son yıllarda bilgi ve bilgisayar güvenliğini zaafa uğratmaya hatta yıkmaya çalışan, kurumlar üzerinde maddi manevi büyük zararlara yol açan, kişi, kurum ve kuruluşları tehdit ederek zararlara uğramasına yol açan bilgi güvenliği tehditlerinin engellenmesi için kurumsal bilgi güvenliği sağlanmalıdır.

Kurumsal bilgi güvenliğini tehdit eden saldırıların bilinmesi, bilgi güvenliğinin sağlanmasına yönelik kurumsal stratejilerin geliştirilmesinde önemli bir role sahiptir. Bilgi sistemlerine yönelik olarak yapılan saldırılar incelendiğinde; saldırıların çok geniş bir yelpazede yapıldığı, otomatik teknikler kullanılarak saldırıların kolayca yapılmasının sağlanmasında önemli artışların görüldüğü tespit edilmiştir. Otomatik saldırı araçları sayesinde kurumsal bilgi güvenliğini tehdit eden usta saldırganların yanında bilinçsiz ve bilgi eksiği olan birçok acemi saldırgan türemiştir. Virüs yazarları, eskiye göre çok daha gelişmiş araçlarla çalışmaktadır. Bu araçları kullanan virüs yazarları, yazılım robotları ve rootkitler, sosyal mühendislik, casusluk ve reklâm amaçlı yazılımlardan yararlanarak karmaşık virüslerle bilgi sistemlerini üst düzeyde tehdit etmektedirler.

Kurumsal bilgi güvenliğinin sağlanması amacıyla, saldırı

türlerinin takip edilmesi, saldırganların kullandığı yöntemlerin saptanması, ülkemizde ve dünyada bu konuda yapılan araştırmaların, raporların ve çalışmalar ile tespit edilen açıkların takip edilmesi ve giderilmesi bilgi güvenliği ihlalinin yaşanmaması için gerekli önlemlerin zamanında alınması, güvenlik ihlallerine anında müdahale edilerek saldırıların zararlarından en az şekilde etkilenme, felaket anında uygulanabilecek felaket ve iş sürekliliği planlarının uygulanması gibi stratejiler, kurumlar tarafından uygulanmalıdır.

Ülkemizde genellikle güvenlik politikaları standartlara uygun olmadan yazılı veya sözlü, onaylı veya onaysız bir biçimde kuruluşlar tarafından uygulanmakta ve çoğu kurum tarafından da bilgi güvenliği yönetimi için yeterli görülmektedir. Bu yanlış anlamanın giderilmesi için dünya genelinde kabul görmüş ve uygulanabilirliği test edilmiş bilgi güvenliği standartları esas alınarak kuruluşların bilgi güvenliği yönetimi konusunda eksikliklerini gidererek BGYS kurmaları ve belgelendirilmeleri gerekmektedir. BGYS çerçevesinde oluşturulacak güvenlik politikalarına üst yönetim ve tüm çalışanların destek vermesi ve tavizsiz bir şekilde uygulanması, işbirliğinde bulunulan tüm kişi ve kuruluşlarında bu politikalara uyma zorunluluğu, kurumsal bilgi güvenliğinin üst düzeyde sağlanmasında önemli bir faktördür.

Kurumsal Bilgi güvenliği standartlarının yüksek seviyede bir güvenlik sağlanmasında etkili olduğu muhakkatır. Bunun ötesinde de sistemlerde açıklar olabileceği, özellikle web uygulamalarında daha dikkatli olunması gerektiği, yeni eğilim ve yaklaşımların keşfedildikçe kurumsal güvenliğinin arttırılması yönünde hayata geçirilmesi gerektiği de asla unutulmamalıdır.

KAYNAKLAR

[1] Thow-Chang, L., Siew-Mun, K., and Foo, A., "Information Security Management Systems and Standards" Synthesis Journal, 2(2):5,8 (2001).
[2] Stytz, M. R., Banks, S.B., "Dynamic software security testing", Security & Privacy Magazine IEEE , 4(3): 77, (2006).
[3] McGraw, G., "Software security", Security & Privacy Magazine IEEE, 2(2): 80 - 81, (2004).
[4] İnternet: CERT "CERT/CC Statistics 1988-2006" http://www.cert.org/stats/ (19.09.2007).
[5] Kudat, B., "Kötü adamların hızına yetişen daha güvenli", BThaber, 604:15, (2007).
[6] Vural, Y., "Kurumsal Bilgi Güvenliği ve Sızma Testleri", Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, 15-20, (2007).
[7] Munro, K., "Social engineering", Infosecurity Today, 2(3):44, (2005).
[8] Barber, R., "Social engineering: A People Problem?", Network Security, 2001(7):9-1, (2001).
[9] Schmidt, A. H., "Building a mosaic of security for a better world", Security Matters, Aspatore Books, U.S.A., 24-26 (2004).
[10] Türkiye Bilişim Derneği, "E-Devlet Uygulamalarında Güvenlik ve Güvenilirlik Yaklaşımları 4. Çalışma Grubu Sonuç Raporu", TBD Kamu-BİB IV, Ankara, 9, 11, 17, (2005).
[11] Türk Standardları Enstitüsü, "Bilgi güvenliği yönetim sistemleri– Özellikler ve kullanım kılavuzu", TSE-TS 1779- 2, Ankara, 3, (2005).
[12] Mitnick, K. D., Simon, L. W., Wozniak, S., "The Art of Deception: Controlling the Human Element of Security", Wiley Publishing, New York, 17-18 (2003).
[13] İnternet: Wikipedia, "ISO/IEC 27001", http://en.wikipedia.org/wiki/ISO_27001 (19.09.2007)
[14] Kalman, S., "Web Security Field Guide", Cisco Press, Indianapolis, 36, 37 (2003).
[15] İnternet: Wikipedia "BS-7799" http://en.wikipedia.org/wiki/BS_7799 (19.09.2007).
[16] Osborne, M., "How to Cheat at Managing Information Security", Syngress Publishing Inc., Rockland, 90, (2006).
[17] İnternet: BSI "Information Security Management Systems Guidelines for Information Security Risk Management" http://www.bsi-global.com (19.09.2007).
[18] İnternet: International Organization for Standardization-ISO "Overview of the ISO system" http://www.iso.org/iso/en/aboutiso/introduction/index.htm (19.09.2007).
[19] İnternet: International Organization for Standardization-ISO "JTC 1 / SC 27" http://www.iso.org/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeDetailPage.TechnicalCommitteeDetail?COMMID=143 (19.09.2007).
[20] İnternet: Wikipedia "ISO 27000 Series" http://en.wikipedia.org/wiki/ISO_17799 (19.09.2007).
[21] İnternet: ISO 27001 Security "ISO/IEC 27003" http://www.iso27001security.com (19.09.2007).
[22] İnternet: Türk Standardları Enstitüsü "İptal Standard" https://www.tse.org.tr/turkish/abone/StandardDetay.asp?STDNO=31987 (25.10.2007).
[23] Symantec Corp., "Symantec Internet Security Threat Report Trends for July–December 06" Symantec Volume XI, Cupertino, 24-64 (2007).
[24] Gordon, L. A., Loeb, M. P., Lucyshyn, W., Richardson, R., "CSI/FBI, Computer Crime and Security Survey", FBI Computer Security Institute, 1- 26, (2005).
[25] Koç.net Haberleşme Teknolojileri ve İletişim Hizmetleri A.Ş., "Türkiye İnternet Güvenliği Araştırma Sonuçları 2005", Koç.net, İstanbul, 5- 12, (2005).
[26] Jia, X., "Design, Implementation and Evaluation of an Automated Testing Tool for Cross-Site Scripting Vulnerabilities", Yüksek Lisans Tezi, Darmstadt University of Technology (TUD) - Computer Science Department, 2-6 (2006).
[27] Foster, C. J., Osipov, V., Bhalla, N., Heinen, N., "Buffer Overflow Attacks: Detect, Exploit, Prevent", Syngress Publishing Inc., Rockland, 4 (2006).
[28] İnternet: OWASP "About The Open Web Application Security Project" http://www.owasp.org (19.09.2007).
[29] İnternet: Web Application Security Consortium "About Us" http://www.webappsec.org (23.07.2006).
[30] Hansche, S., "Official (ISC2) Guide to the CISSP Exam", Auerbach Publications, New York, 12, (2003).
[31] Endler, D., "Brute-Force Exploitation of Web Application Session IDs", IDEFENSE Labs,Chantilly, 4-5 (2001).
[32] Fu, K., Sit, E., Faemster, N., "DoS and Donts of Client Authentication on the Web" USENIX Security Symposium, Washington, 258-260, (2001).
[33] Kolsek, M., "Session Fixation Vulnerability in Web-based Applications", ACROS Security, Maribor, 2- 4 (2002).