Gazi Üniv. Müh. Mim. Fak. Der.
Cilt 23, No 2, 507-522, 2008

J. Fac. Eng. Arch. Gazi Univ.
Vol 23, No 2, 507-522, 2008

KURUMSAL BİLGİ GÜVENLİĞİ VE STANDARTLARI ÜZERİNE BİR İNCELEME

Yılmaz VURAL ve Şeref SAĞIROĞLU*
STM A.Ş., Mecnun Sok. No:58 Beştepe, 06510 Ankara
*Bilgisayar Mühendisliği Bölümü, Mühendislik-Mimarlık Fakültesi, Gazi Üniversitesi, Maltepe 06570, Ankara
yvural@stm.com.tr, ss@gazi.edu.tr

(Geliş/Received: 17.02.2007; Kabul/Accepted: 18.02.2008)

ÖZET

Bilgi varlıklarının korunabilmesi, kurumların karşılaşabileceği risklerin en aza indirgenmesi ve iş sürekliliğinin sağlanması, Bilgi Güvenliği Yönetim Sistemlerinin kurumlarda üst yönetim desteğiyle hayata geçirilmesiyle mümkün olmaktadır. Kurumsal bilgi güvenliğinin yüksek seviyede sağlanması ile ilgili olarak literatürdeki mevcut kaynaklar araştırılıp incelendiğinde, kapsamlı ve güncel bir çalışma olmadığı, sunulan çalışmaların yeterli olmadığı, çoğunlukla ticari içerikli veya güvenilir olmayan web sitelerinde yer aldığı ve nasıl korunması gerektiğiyle ilgili kısa bilgilere yer verildiği tespit edilmiştir. Bu çalışmada genel olarak kurumsal bilgi güvenliği incelenmiş ve değerlendirilmiştir. Mevcut bilgi güvenliği standartları ile yeni oluşturulmakta olan bilgi güvenliği standartları da bu çerçevede gözden geçirilmiştir. Bu tespitlerden yola çıkarak bu çalışmada, kurumsal bilgi güvenliğinin yüksek seviyede sağlanması ve ülkemizde kurumsal bilgi güvenliği bilincinin geliştirilmesi için kurumlar ve bireylerin bilgilendirilmesi amaçlanmıştır. Bu çalışmanın, kurumsal bilgi güvenliğinin yüksek seviyede sağlanmasına yönelik farkındalık oluşturması, mevcut ve yeni standartlar hakkında daha fazla bilgi içermesi, literatür özetini sunması ve yüksek seviyede güvenliğin sağlanmasına katkılar sağlayacağı düşünülmektedir.

Anahtar Kelimeler: Bilgi güvenliği, kurumsal bilgi güvenliği, bilişim güvenliği, güvenlik politikaları, bilgi güvenliği standartları, bilgi güvenliği yönetim sistemleri.

A REVIEW ON ENTERPRISE INFORMATION SECURITY AND STANDARDS

ABSTRACT

Information assests are very important for enterprises. In order to secure these assests, risks should be reduced, availability should be enabled, and information secuirty management system should be supported by executives. When the literature has been 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. As a result of those, a review study on enterprises security and standards has been presented in this study. It was concluded that this study would increase security awareness, give details about new standards, conclude the available documents and suggest some issues for enterprises willing to improve their security.

Keywords: Information security, enterprise information security, IT security, security policies, information security standards, information security management system.

1. GİRİŞ (INTRODUCTION)

İletişim ortamlarının yaygınlaşması ve kullanımının artması sonucunda elektronik ortamlarda bulunan bilgilerin her geçen gün katlanarak artmasından dolayı bilgi güvenliğinin sağlanması ihtiyacı kişisel veya kurumsal olarak en üst seviyelere çıkmıştır. Bunun önemli sebepleri iş veya günlük yaşamın bir parçası haline gelen elektronik uygulamaların artması, ihtiyaç duyulan bilgilerin ağ sistemleri üzerinde

paylaşımı, bilgiye her noktadan erişilebilirlik, bu ortamlarda meydana gelen açıkların büyük tehdit oluşturması ve en önemlisi kişisel ve kurumsal kayıplarda meydana gelen artışlar olarak sıralanabilir. Kişi ve kurumların bilgi güvenliğini sağlamadaki eksikliklerinin yanında saldırganların saldırı yapabilmeleri için ihtiyaç duydukları yazılımlara internet üzerinden kolaylıkla erişebilmeleri fazla bilgi birikimine ihtiyaç duyulmaması ve en önemlisi ise kişisel ve kurumsal bilgi varlıklarına yapılan saldırılardaki artışlar, gerek kişisel gerekse kurumsal bilgi güvenliğine daha fazla önem verilmesine yeni yaklaşımların ve standartların kurumlar bünyesinde uygulanması zorunluluğunu ortaya çıkarmıştır.

Kurumsal bilgi güvenliği, bilginin üretildiği, işlendiği ve saklandığı her ortamda sağlanmak zorundadır. Bunun için mevcut yazılımlar, donanımlar, ortamlar ve insan kaynakları dikkate alınmalıdır. Bilginin korunmasına çalışıldığı ilk günden itibaren güvenlik zincirinin en zayıf halkasını her zaman insanlar oluşturmuşlardır [1]. Birçok teknik veya teknik olmayan güvenlik kontrolleri uygulansa dahi bu kontroller saldırganlar tarafından en zayıf halka olan insan faktörü kullanılarak çeşitli yöntemlerle aşılabilmektedir. Genel bir söylem olan "gücünüz en zayıf halkanız kadardır" ilkesi bilgi güvenliği içinde geçerlidir [2]. Yapılan çalışmalarda [1-7] bilgi güvenliği açıkları ve kayıplarının artması sebebiyle bu konunun henüz doğru olarak anlaşılmadığı, gereken önemin verilmediği ve bilinçlenmenin gereken seviyede olmadığını bizlere göstermektedir.

2005 yılında yaygın olarak kullanılan ve 2006 yılının son aylarına damgasını vuran ve günümüzde hala popüler olan sazan avlama (phishing) saldırganlar tarafından kullanılan etkili bir saldırı yöntemidir. Geçmiş yıllarda bilgi sistemlerine en büyük zararları veren virüsler 2006 yılı itibariyle yerlerini casus programların sazan avlama yöntemiyle kullanıldığı saldırılara bırakmıştır. Dünyada olduğu gibi ülkemizde de sıkça karşılaşılan bu yöntemde genellikle bilgi güvenliği bilinci olmayan kullanıcılar kurban olarak seçilmekte ve internet bankacılığı odaklı soygunlar yapılmaktadır. Sazan avlama çalışma grubu (Anti-Phishing Working Group) tarafından Temmuz 2006 tarihinde yayınlanan aylık rapora göre 14,191 web sitesi üzerinde kimlik hırsızlığı, soygun ve diğer kötücül amaçlar için kullanılan 23,670 tekil sazan avlama vakası tespit edilmiştir [4]. Netcraft firması tarafından geliştirilen ve web tarayıcılarıyla bütünleşik olarak çalışan güvenlik yazılımı sayesinde sazan avlama saldırıları konusunda yapılan incelemelerde 2005 yılında 41.000 olan saldırı sayısının 2006 yılı sonunda 609.000'e çıktığı gözlemlenmiştir [5]. Dünyaca ünlü güvenlik firması tarafından verilen bu rakamlar tehlikenin hangi hızla ilerlediğinin gösterilmesi açısından önemlidir. Sazan avlama konusunda Messagelabs firması tarafından yapılan bir başka araştırmada Netcraft firmasının sonuçlarını desteklemektedir. Ocak 2006 tarihi itibariyle %10,6 olan sazan posta oranı Aralık 2006 sonu itibariyle %68,6 gibi yüksek bir rakama çıkmıştır. Bu artışın 2005 yılı genelinde %13,1 olduğu göz önüne alındığında 2006 yılındaki rakamın ne kadar büyük olduğu görülmektedir [6].

Ülkemizde sazan avlama ve benzeri saldırı teknikleriyle ilgili araştırmalar yapılmadığından, bu konuda istatistikler verilememiştir. Ancak bu tür araştırmaların bilgi güvenliğine önem veren gelişmiş ülkelerde yapıldığını (A.B.D. İngiltere, Avustralya, vb.) göz önüne alırsak ülkemizde durumun daha da kötü olduğu ortaya çıkacaktır. Buradan da anlaşılacağı gibi önümüzdeki yıllarda çok yüksek teknik bilgiler üzerine kurulu saldırılardan ziyade bilgi güvenliği bilincine haiz olmayan kişilerin kandırılması sonucunda ortaya çıkan güvenlik açıklarının saldırganlar tarafından ustaca kullanılacağı tahmin edilmektedir.

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 [7]. 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 [7].

Literatürde yaşanan önemli olaylardan görüleceği üzere kurumsal bilgi güvenliğinin üst seviyede sağlanabilmesi için bilgi güvenliğinin devamlılık gerektiren bir süreç olduğu ve bu sürecin kurumsal bilgi güvenliği standartları çerçevesinde yönetilmesi gerektiği unutulmamalıdır. Sazan avlama saldırılarıyla kullanıcıların kandırılmasını önlemenin yegâne yolunun kurumsal bilgi güvenliği yönetim sistemleri çatısı altında yapılacak olan eğitim ve bilinçlendirme çalışmalarının olduğu unutulmamalıdır.

Bu çalışmanın amacı; kurumsal bilgi güvenliğini genel olarak incelemek, mevcut çalışmaları özetlemek, kurumsal bilgi güvenliğinin kurumlarda etkin bir şekilde hayata geçirilmesinin önemini vurgulamak, kurumsal bilgi güvenliğinin etkin bir şekilde hayata geçirilmesinde önemli bir yer tutan ISO tarafından yeni yayınlanan ve hali hazırda geliştirilmekte olan ISO/IEC 27000 serisi standartlarını kısaca sunmak, ülkemizde konuya daha çok önem verilmesini sağlamak ve kurumsal bilgi güvenliğinin önemini güncel açıdan değerlendirmek, kurumsal bilgi

güvenliğinin üst seviyede sağlanmasına yönelik güncel tehditler ve eğilimleri incelemek, konunun önemini bir kez daha vurgulamak ve konuya tekrar dikkat çekmek, ülkemizde bu alanda yayınlanmış kapsamlı bir makale olmamasından dolayı bu konudaki bilgi açığını kapatmak, konuya geniş bir açıdan bakarak bu konudaki farkındalığını daha da artırmak, yüksek seviyede kurumsal bilgi güvenliğini tehdit eden önemli açıkları tespit etmek ve giderilmesine yönelik öneriler sunmak olarak sıralanabilir.

Konunun daha iyi anlaşılması ve gerekli tedbirlerin doğru bir şekilde alınabilmesi için Bölüm 2'de kurumsal bilgi güvenliği tanımı ve kapsamı verilmiştir. Bölüm 3'de ise kurumsal güvenlik için oluşturulması ve uygulanması gereken güvenlik politikaları açıklanmıştır. Bölüm 4'de bilgi güvenliğinin doğru bir şekilde yürütülebilmesi için gerekli olan kapsam özetlenmiştir. Bilgi güvenliğinin yüksek seviyede sağlanmasında temel unsurlarından olan uluslararası standartlar Bölüm 5'de tanıtılmıştır. Bu bölümde ayrıca ülkemizde bu konuda yapılan çalışmalarda sunulmuştur. Son bölümde ise bu çalışmada sunulan hususlar değerlendirilmiş ve yüksek seviyede kurumsal bilgi güvenliğinin sağlanmasındaki önemli unsurlar değerlendirilmiş ve öneriler sunulmuştur.

2. KURUMSAL BİLGİ GÜVENLİĞİ (ENTERPRISE INFORMATION SECURITY)

Kişilerin bilgi güvenliği önem arz ederken, bundan daha önemlisi, kişilerin güvenliğini doğrudan etkileyen kurumsal bilgi güvenliğidir. Her birey bilgi sistemleri üzerinden hizmet alırken veya hizmet sunarken kurumsal bilgi varlıklarını doğrudan veya dolaylı olarak kullanmaktadır. Bu hizmetler kurumsal anlamda bir hizmet alımı olabileceği gibi, bankacılık işlemleri veya bir kurum içerisinde yapılan bireysel işlemler de olabilir. Kurumsal bilgi varlıklarının güvenliği sağlanmadıkça, kişisel güvenlikte 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 [8]. 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 güvenliği insan faktörü, eğitim, teknoloji gibi birçok faktörün etki ettiği tek bir çatı altında yönetilmesi zorunlu olan karmaşık süreçlerden oluşmaktadır. Bu süreçlerin yönetilmesi, güvenlik sistemlerinin uluslararası standartlarda yapılandırılması ve yüksek seviyede bilgi güvenliğinin sağlanması amacıyla tüm dünyada kurumsal bilgi güvenliğinin yönetiminde standartlaşma çalışmaları 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 [9].

Ülkemizde Avrupa Birliği Uyum Kriterlerinde de adı geçen bu standartların uygulanması konusunda yapılan çalışmalar yetersiz olup bu standardı uygulayan kurum ve kuruluşların sayısı yok denecek kadar azdır. ISO–27001:2005 standardı ülkemizde Türk Standardları Enstitüsü (TSE) tarafından TS ISO/IEC 27001 "Bilgi Güvenliği Yönetim Sistemi" standardı adı altında yayınlanmış ve belgeleme çalışmaları başlatılmıştır. Bu standart kapsamında kurumsal bilgi varlıklarının güvenliğinin istenilen düzeyde sağlanabilmesi amacıyla; gizlilik, bütünlük ve erişilebilirlik gibi güvenlik unsurlarının kurumlar tarafından sağlanması gerekmektedir.

Bilgi Güvenliği Yönetim Sistemleri (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 güvenlik politikalarının oluşturulması, BGYS kapsamının belirlenmesi, risk yönetimi, denetim kontrollerinin seçilmesi, uygulanabilirlik beyannameleri BGYS kurulabilmesi için, yapılması gereken adımlardır [10]. Bilgi güvenliğinin yönetiminin kurulmasında izlenmesi gereken adımlar bu bölümde sırasıyla takip eden başlıklarda açıklanmıştır.

3. KURUMSAL BİLGİ GÜVENLİĞİ POLİTİKALARI (ENTERPRISE INFORMATION SECURITY POLICIES)

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 [11]. 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 tüm çalışanların

uyması gereken kuralları içeren belgelerdir. Bilgi güvenliği politikaları her kuruluş için farklılık göstersede 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 ifadeleri içermektedir.

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 oluşur [11]. Kurumsal Güvenlik Politikası içerisinde bulunması gereken bölümler Tablo 1'de özetlenmiştir.

Belirli konularda çalışanın daha fazla bilgilendirilmesi,dikkat etmesi gereken hususlar, ilgili konunun detaylı bir şekilde ifade edilmesi istendiğinde alt politikalar geliştirilmelidir. Örneğin kullanıcı hesaplarının oluşturulması ve yönetilmesi, şifre unutma, şifre değiştirme, yeni şifre tanımlama gibi durumlarda uyulacak kurallar alt politikalar aracılığıyla açıklanmalıdır.

Tablo 1. Güvenlik politikası kısımları

Bölüm Adı	İçeriği
Genel Açıklama	Politikayla ilgili gerekçeler ve buna bağlı risklerin tanımlamasını kapsar.
Amaç	Politikanın yazılmasındaki amaç ve neden böyle bir politikaya ihtiyaç duyulduğunu açıklar.
Kapsam	Politikaya uyması gereken çalışan grupları (ilgili bir grup veya kurumun tamamı) ve bilgi varlıklarını belirler.
Politika	Uygulanması ve uyulması gereken kuralları veya politikaları içerir.
Cezai Yaptırımlar	Politika ihlallerinde uygulanacak cezai yaptırımları açıklar.
Tanımlar	Teknik terimler ile açık olmayan ifadeler listelenerek açıklanır.
Düzeltme Tarihçesi	Politika içerisinde yapılan değişiklikler, tarihler ve sebepleri yer alır.

E-posta gönderme ve alma konusunda, üst yönetimin kararlarını, kullanıcının uyması gereken kuralları ve diğer haklarını alt politika içerisinde ifade etmek bir başka örnek olarak verilebilir. 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, bilgisayarlarda uygulanacak erişim denetim ölçütleri, güvenlikle ilgili kullanılan yazılım ve donanımların nasıl kullanılacağı gibi konular da açıklanabilir.

Kurumsal bilgi güvenliği politikaları kuruluşların ihtiyaçları doğrultusunda temel güvenlik unsurlarının (gizlilik, bütünlük, erişilebilirlik, vb.) bazıları üzerinde yoğunlaşabilir. Örneğin askeri kurumlarda, bilgi güvenliği politikalarında gizlilik ve bütünlük unsurları ön plana çıkmaktadır. 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 kurumlarda uygulanan bilgi güvenliği politikalarında genellikle erişilebilirlik ve bütünlük unsurları ön planda gelmektedir. Üniversite sınav sonuçlarının açıklandığı yükseköğretim kurumunda 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 politikaları 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.

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.

4. BGYS KAPSAMI (BGYS SCOPE)

BGYS'nin kapsamı kurumların sahip olduğu bilgi varlıkları ve ihtiyaçları doğrultusunda tespit edilir. Bu kapsam

- Kurumun sahip olduğu bilgi varlıklarının tamamı,
- Bilgi sistemlerinin bir kısmı (Bilişim sistemleri, kâğıt ortamdaki bilgiler, elektronik bilgi varlıkları, vb.),
- Belli bir yerleşim birimindeki bilgi sistemleri (Merkez binalar, Genel Müdürlükler, vb.),
- Odaklanılmış bir bilgi sistemi (bilgisayarlar, ağ sistemi, sunucu bilgisayarlar, web sunucusu, vb.)

olabilir [10].

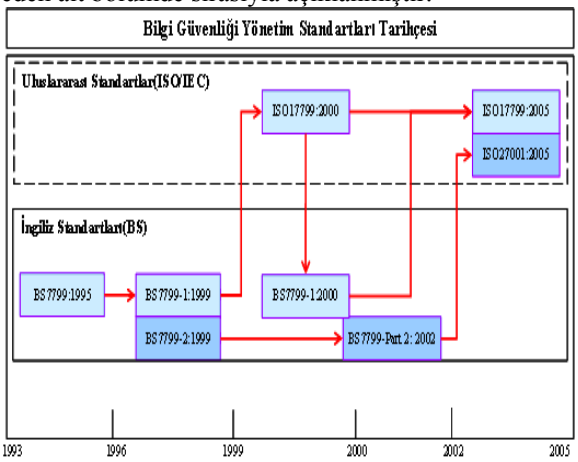
Bir kuruluşta elektronik ortamlarda üretilen, dağıtılan ve saklanan bilgiler BGYS kapsamına örnek olarak verilebilir.

5. BİLGİ GÜVENLİĞİ STANDARTLARI (INFORMATION SECURITY STANDARDS)

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 yapılan çalışmalar sonucunda İngiliz Standartlar Enstitüsü (British Standards Institute-BSI) tarafından 1995 yılında BS–7799 standardının ilk kısmı olan BS7799–1, 1999 yılında ise aynı standardın ikinci kısmı olan BS7799–2 İngiliz standardı olarak yayınlanmıştır.

BS7799–1 2000 yılında küçük düzeltme ve adaptasyonlardan geçerek ISO tarafından ISO/IEC–17799 adıyla kabul edilmiş ve dünya genelinde kabul edilen bir standart halini almıştır. 2002 yılında ise BSI tarafından BS–7799 standardının ikinci kısmı olan BS–7799–2 standardı üzerinde eklemeler ve düzeltmeler yapılarak ikinci defa İngiliz standardı olarak yayınlanmıştır. 2005 yılında ise ISO tarafından ISO/IEC–17799 standardı üzerinde eklemeler ve düzeltmeler yapılmış ISO/IEC–17799:2005 adıyla yeniden yayınlanmıştır. Son olarak 2005 yılında ISO İngiliz standardı olan BS7799–2 üzerinde eklemeler ve düzeltmeler yaparak ISO/IEC:27001 standardını yayınlamıştır [12]. Bilgi güvenliği yönetim sistemlerinin temelini teşkil eden standartların yayınlanma süreleri Şekil 1'de tarihsel akışa göre verilmiştir.

Şekil 2'de verilen ve kurumsal bilgi güvenliğinin üst düzeyde sağlanması için gerekli olan bilgi güvenliği yönetiminde kullanılan uluslararası standartlar takip eden alt bölümde sırasıyla açıklanmıştır.



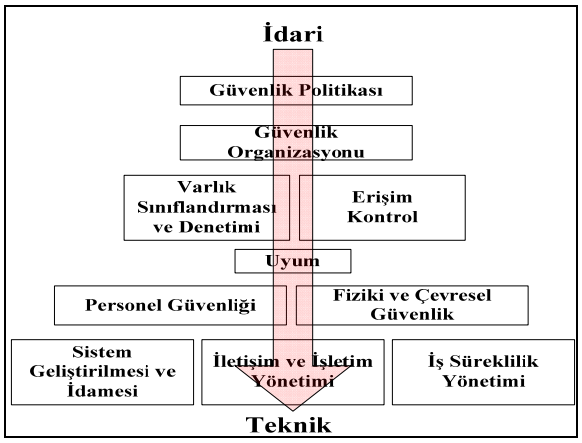
Şekil 1. Standartların yayınlanma süreleri

5.1. İngiliz Standartları (British Standards)

BS–7799, bilgi varlıklarının gizlilik, doğruluk ve erişilebilirliğini güvence altına almak için uygulanması gereken güvenlik denetimlerini düzenleyen ve belgelendiren iki aşamalı İngiliz standardıdır. 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. BS–7799 standardı endüstri, devlet ve ticari kuruluşlardan ortak bir güvenlik modeli oluşturulmasına gelen talepler sonucu BSI kuruluşu ve BOC, BT, Marks&Spencer, Midland Bank, Nationwide Building Society, Shell, Unilever ve diğer bazı şirketlerin katılımıyla hazırlanmış bir standarttır. 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 [13].

BS–7799 standardı teknik ve idari bölümlerden oluşmaktadır. Standardın birinci kısmının ilk sürümünde yer alan etki alanlarının idari ve teknik kısımlara göre sınıflandırılması Şekil 2'de gösterilmiştir. Etki alanları aşağıda maddeler halinde özetlenmiştir [14].



Şekil 2. BS–7799 (Sürüm–1) bölümleri

Güvenlik politikası: Bilgi güvenliği için yönetimin yönlendirilmesi ve desteğinin sağlanmasının yer aldığı bölümdür.

Güvenlik organizasyonu: İşletme içindeki bilgi güvenliğinin yönetilmesi, üçüncü taraflarca erişilen işletmeye ait bilgi işleme araçlarının ve bilgi varlıklarının güvenliğinin korunması ve bilgi işleme sorumluluğu başka bir işletmenin kaynaklarından sağlandığında bilgi güvenliğinin sürdürülmesidir.

Varlık sınıflandırması ve denetimi: İşletmeye ait varlıklar için uygun korunmanın sağlanması ve bilgi kaynaklarının uygun koruma seviyesine sahip olduklarının garanti edilmesidir.

Erişim kontrol: Bilgiye erişimin denetlenmesi, bilgi sistemlerine yetkisiz erişimin engellenmesi, yetkisiz kullanıcı erişimine izin verilmemesi, hizmetlerin korunması, yetkisiz işlemlerin tespit edilmesi ve uzaktan çalışma ortamlarında bilgi güvenliğinin sağlanmasıdır.

Uyum: Herhangi bir suçtan kaçınılması, organizasyonun güvenlik politikalarının ve standartlarının sisteme uyumunun sağlanması, sistem izleme işlemlerinin etkisinin artırılması ve karşılaşılan engellerin azaltılmasıdır.

Personel güvenliği: İnsan hatalarını, hırsızlığı, sahtekârlığı ve araçların yanlış kullanılması risklerinin azaltılması, kullanıcıların bilgi güvenliği tehditlerinden ve sorunlarından haberdar olduklarının ve normal çalışma seyirleri içinde organizasyonla ilgili güvenlik politikasını desteklemek üzere donatıldıklarının garanti edilmesidir. Ayrıca güvenlik ihlallerinden meydana gelen hasarın en aza indirilmesi ve bu gibi olaylardan gerekli tecrübelerin edinilmesidir.

Fiziki ve çevresel güvenlik: İşyerine yetkisiz erişimlerin engellenmesi ve bilgi varlıklarının hırsızlığa veya tehlikeye karşı korunmasıdır.

Sistem bakım ve idamesi: Bilişim sistemleri içerisinde güvenliğin temin edilmesi, uygulama sistemlerindeki kullanıcı verilerinin kaybedilmesini, değişmesini ya da hatalı kullanımının önlenmesi, bilginin gizliliği, aslına uygunluğu ya da bütünlüğünün korunması, IT projelerinin ve destek etkinliklerinin güvenli bir şekilde yürütülmesini temin etmek ve uygulama yazılımının ve bilgilerin güvenliğini sağlamaktır.

İletişim ve işletim yönetimi: Bilgi işlem tesislerinin doğru ve güvenle işletildiğinden emin olunması, sistem arızalarını en az seviyeye indirilmesi, bilgi ve yazılım bütünlüğünün korunması, bilgi işlem ve iletişim hizmetlerinin kullanılabilirliği ve bütünlüğünün sürdürülmesi, ağlarda yer alan bilgilerin emniyetinin ve destekleyen altyapı sisteminin korunması, iş faaliyetlerinin kesintiye uğratılması ve varlıklara zarar verilmesinin önlenmesi ve organizasyonlar arasında akan bilginin yanlış amaçlarla kullanılması, değiştirilmesi ve kaybedilmesinin önlenmesidir.

İş süreklilik yönetimi: Ticari süreçlerde karşılaşılan olumsuzlukların giderilmesi ve kritik ticari işlemlerin devamlılığının sağlanmasıdır.

Kurumlar bilgi varlıklarını tespit edip sınıflandırdıktan sonra, bilgi varlıklarına yönelik tehditleri ve zafiyetleri değerlendirerek yukarıda anlatılan kontrollerden hangilerinin uygulanıp, hangilerinin uygulanamayacağına karar vererek standardın kapsamını kendi kurumlarına özgü bir şekilde belirleyebilmektedirler.

BS–7799 ikinci kısmında kurumsal güvenlik ihtiyaçlarının belirlenmesi için gerekli olan bilgi güvenliği yönetiminin çatısı tanımlanarak BS–7799 birinci kısmında tanımlanan kontroller uygulanmaktadır. Bu standart, yöneticilere ve personele etkin bir BGYS kurmaları ve yönetmeleri açısından bir model sağlamak üzere hazırlanmıştır. Bu modelde "Planla– Uygula–Kontrol Et–Önlem Al (PUKÖ)" adımları bulunmaktadır. Bu modelin basamakları ISO standartları bölümünde açıklanmıştır.

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 kaynaklar, terimlerin

tanımı, kurum bağlamında risk, risk değerlendirmesi, risk kararının verilmesi, risk yönetimi BS7799–3 standardının bölümlerini oluşturmaktadır [15].

5.2. ISO/IEC Standartları (ISO/IEC Standards)

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, İsviçre'nin Cenova şehrinde kurulmuştur. 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 SC27: BT Güvenlik Teknikleri Alt Komisyonunda ele alınmaktadır. Bilgi güvenliği konusunda çalışan bu komisyonun sorumluluklarından bazıları aşağıda belirtilmiştir [16]. Bu sorumluluklar;

- Bilgi teknolojileri sistemleri güvenlik hizmetlerinin ve ihtiyaçların tanımlanması,
- Güvenlik teknikleri ve mekanizmalarının geliştirilmesi,
- Güvenlik kılavuzlarının geliştirilmesi ve
- Yönetim destek dokümanları ile standartların geliştirilmesidir.

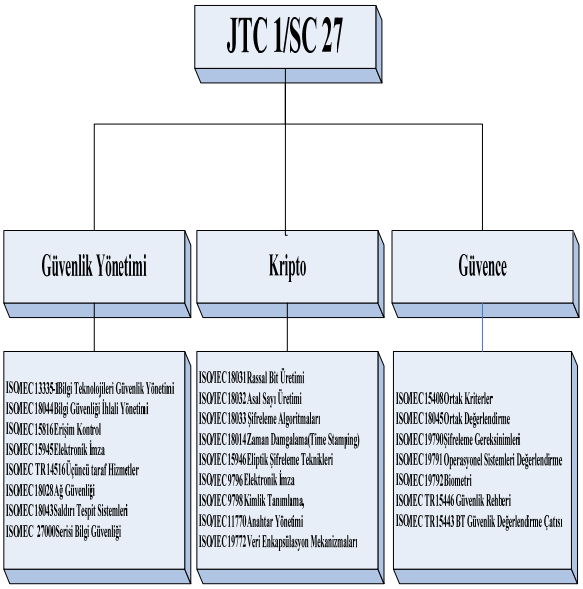
Yukarıda açıklanan görevleri yerine getirmek üzere bu komisyon içinde 5 ayrı çalışma grubu (Working Group) bulunmaktadır. Bu gruplar aşağıda belirtilmiştir.

- 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

1, 2 ve 3 nolu çalışma grupları ve sorumlu oldukları konular Şekil 3'de gösterilmiştir.

SC27'ye bağlı çalışma gruplarından Çalışma Grubu–1 (WG-1), Şekil 3'de gösterilen bilgi güvenliği yönetim sistemleri standartları (ISO/IEC 17799, ISO/IEC 27000 Serisi) ile ilgili çalışmaları yürütmektedir. Bu standartlar aşağıda kısaca açıklanmıştır.

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/IEC 17779 standardı daha önceki bölümde açıklanan BS–7799 standardının ilk bölümüne eşdeğerdir. Tablo 2 standartların kullanımı ile ilgili seçenekleri göstermektedir.



Şekil 3. ISO/IEC güvenlik çalışma grupları

Tablo 2. Standart kullanım amaçları

Şirket Tipi	Çalışan	Amaç
Küçük	<200	Bilinçlendirme
Büyük	>200	Sertifika almak

ISO/IEC 17799 standardının uygulanmasıyla kurumsal bilgilerin tamamen güvende olduğunu söylemek doğru değildir. Bu standart bilgi güvenliğini başlatan, gerçekleştiren ve sürekliliğini sağlayan kurumların kullanımı için, bilgi güvenlik yönetimi ile ilgili tavsiyeleri kapsar. ISO/IEC 17799 güvenlik standartlarını bir kurumun uyguluyor olması kurumlara aşağıda sıralanan üstünlükleri sağlamaktadır [17].

- *Organizasyon Seviyesinde,* sorumlulukları belirleyerek, kurumsal bilgi güvenliğinin her seviyede uygulanmasının yararlarını garanti eder.
- *Kanuni Seviyede,* kurumun ilgili tüm kural ve yönetmeliklere uyduğunu yetkili makamlara göstererek diğer standart ve mevzuatları tamamlar.
- *İşletme Seviyesinde,* Bilgi sistemleri, zafiyetleri ve nasıl korunacakları konusunda işletmenin yönlendirilmesini sağlayarak kurumsal bilgi sistemlerine daha güvenli erişim sağlanır.
- *Ticari Seviyede,* iş ortakları, hissedarlar ve müşteriler; kurumun bilgi koruması konusuna verdiği önem sayesinde kuruma olan güvenleri artırır ve ticari rakipleri arasında piyasada farklı bir yere gelmesini sağlar.
- *Finansal Seviyede,* güvenlik açıklarının belirlenerek önlem alınması sonucunda maliyetler azalacaktır.

- *Çalışan Seviyesinde,* çalışanın güvenlik konuları ve organizasyon içinde kendisine düşen sorumluluk hakkındaki bilgisini arttırarak bireysel olarak bilinçlendirilmesini sağlar.

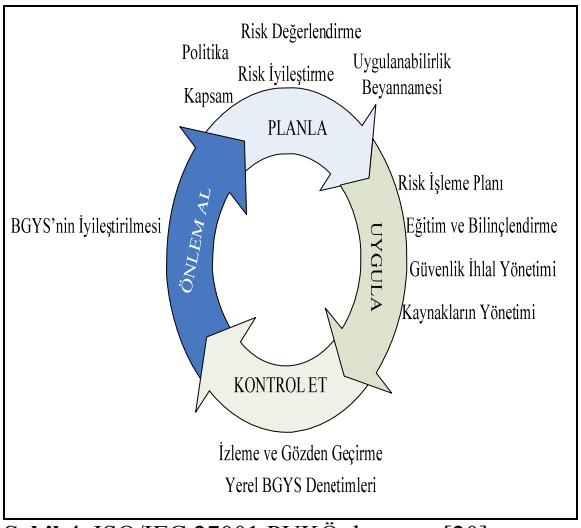
ISO/IEC 17799 standardı 2005 yılında gözden geçirilerek ISO/IEC 17799:2005 ismiyle son halini almıştır. ISO/IEC 17799:2005 Bilgi Güvenliği Yönetimi için uygulama kodu, kuruluşların bilgi güvenliği yönetim sistemini kurmaları, uygulamaları, sürdürmeleri ve iyileştirmeleri için hazırlanmış bir kılavuz olup önceki sürümünden farklı olarak, yaşanan problemlerden, arızalardan, kazalardan ders çıkarılması ve tekrar yaşanmaması için gerekli önlemlerin alınması için gerekli olan yönetim mekanizmasının kurulmasını sağlayan Bilgi Güvenliği İhlallerinin yönetimi ile ilgili bilgi güvenliği denetimlerini ve ilgili uygulamaları da içermektedir [18]. ISO, 2005 yılında bir düzenlemeye giderek Çizelge 5.2'de verilen 27000 serisini bilgi güvenliği için kullanma kararı almıştır [19]. ISO/IEC 27000-27059 arasındaki standartlar ISO tarafından SC27 grubuna dâhil çalışma grupları için bilgi güvenliğiyle ilgili planlanan standartlara ayrılmıştır.

Tablo 3'de kısaca açıklanan standartların tamamı yayınlanarak kullanıma açılmamıştır. Yayınlanan standarda ek olarak geliştirme ve düşünce aşamasında olan standartlara ait açıklamalar aşağıda verilmiştir.
ISO/IEC 27000, bilgi güvenliği serisinde yer alan standartlar içerisinde geçen teknik terimler ve açıklamalarının yer aldığı genel bir sözlük formatında geliştirilmektedir.

Tablo 3. ISO 27000 serisi standartları

Standart No	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)

ISO/IEC 27001, BGYS için gereklilikleri ortaya koyan bir standarttır. Daha öncede anlatıldığı gibi bilgilerin düzenli olarak maruz kaldığı tehditlerin tanımlanmasına, yönetilmesine ve bunların minimize edilmesine yardımcı olur.



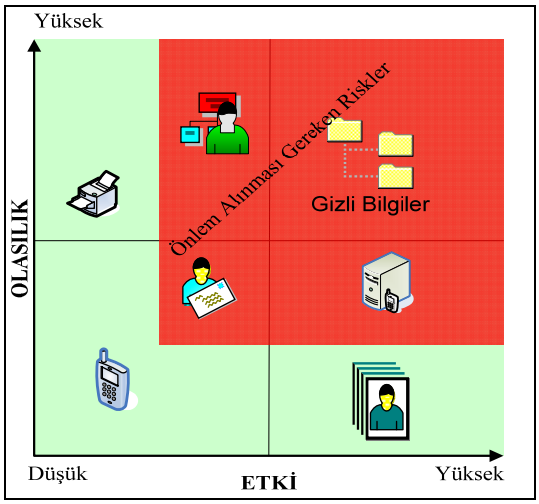
Şekil 4. ISO/IEC 27001 PUKÖ döngüsü [20]

Bu standart; yönetim standartlarıyla (ISO 9001, ISO 14001) uyumlu olarak geliştirildiğinden yönetim standartlarının gereklerini de yerine getirmektedir. ISO/IEC 27001 standardının PUKÖ döngüsü Şekil 4'de gösterilmiş ve kısaca aşağıda açıklanmıştır [20]. Bunlar;

- Kapsam, daha önceki bölümlerde açıklandığı gibi kurumun tamamı veya belirli bir kısmını veya belirli bir hizmetini (internet bankacılığı, web uygulamaları, vb.) içerebilir.
- Politika, Bilgi güvenliği neden önemlidir? Tehditler nelerdir? Risk yönetimi nasıl yapılmalıdır? Uyulması gereken kısıtlar (kanunlar yönetmelikler, vb.) nelerdir? Bu gibi soruların cevabını içeren üst yönetici tarafından onaylanan bilgi güvenliği politikasının bir üst kümesi olarak kabul edilen kısa dokümanlardır.
- Risk Değerlendirme, hangi bilgi varlıklarının korunacağı belirlendikten sonra kuruluşa uygun risk değerlendirme yönteminin seçilerek risklerin tanımlanması yapılır. Seçilen risk değerlendirme yöntemine göre bilgi varlıkları Şekil 5'de örneği gösterilen risk haritasında konumlandırılır. Değerlendirilme yapıldıktan sonra risk değerlendirme haritasında, etkisi ve olasılığı yüksek olan tehditler için risklerin iyileştirilerek kontrol altına alınması işlemlerini kapsar. Risk haritasında bilgi varlıklarının yeri değişebileceğinden risk değerlendirme haritası düzenli olarak güncellenmeli ve gerekli önlemler alınmalıdır.
- Risk İyileştirme, risklerin değerlendirilmesi tamamlandıktan sonra ISO/IEC 27001 standardı risklerin nasıl iyileştirileceğinin açıklanmasını ister. İyileştirme çalışmaları kapsamında risk kabul

edilebilir, transfer edilebilir (sigorta, vb.) azaltma çalışmaları yapılabilir. Riskler karşısında alınması gereken önlemlerin bulunduğu dokümanlar risk iyileştirme planlarını oluşturmaktadır.

•



Şekil 5. Risk değerlendirme haritası

• Uygulanabilirlik Beyannamesi, (Statement of Applicability-SOA), ISO/IEC 27001:2005 standardındaki kontrollerden hangilerinin kullanılıp kullanılmadığını gerekçeleriyle açıklayan belgelerdir. Kullanılan kontrollerin seçilme gerekçeleri, kullanılmayan kontrollerin dışarıda bırakılmasının açıklamasını içerir. Kullanılmayan kontrollerin yanlışlıkla çıkarılmadığının çapraz denetimini sağlar. Uygulanabilirlik beyannamesi risk yönetimini ilgilendiren kararların özetini içerir.

• Risk İşleme Planı, güvenlik risklerini yönetmek için uygun yönetim eylemini, kaynaklarını, sorumluluklarını ve önceliklerini tanımlar. Seçilen kontrollerin yapılabilmesi için gerekli olan alt kontroller gerçekleştirilir ve kontrollerin etkinliği ölçülür.

• Eğitim ve Bilinçlendirme, programlarıyla kurumdaki tüm personelin bilgi güvenliği faaliyetlerinin yarar ve öneminin farkında olarak, BGYS'nin amaçlarına ulaşılmasına nasıl katkı sağlayacağının farkında olması sağlanmalıdır. Ayrıca BGYS'yi teknik olarak etkileyecek işlerde çalışmak üzere uzman personel istihdam edilmesi veya ilgili personelin eğitimleri bu kapsamda yapılır.

• Güvenlik İhlal Yönetimi, güvenlik olaylarının anında tespit edilerek güvenlik ihlâllerine zamanında cevaplar verilmesini sağlar. Daha önce denenen ve başarılı olan güvenlik kırılmaları, güvenlik yöneticisinin güvenlik faaliyetlerinin beklenen biçimde çalışıp çalışmadığının belirlenebilmesi, güvenlik önlemlerinin alınarak güvenlik ihlallerinin önlenmesi, bir güvenlik kırılmasını önlemek için alınan önlemlerin etkili olup olmadığına karar verilir.

• Kaynakların Yönetimi, BGYS'yi kurma, gerçekleştirme, işletme, izleme, gözden geçirme, sürekliliğini sağlama ve iyileştirme için gereken kaynaklar kurum tarafından sağlanarak yönetimi yapılmalıdır.

• İzleme ve Gözden Geçirme, BGYS'nin etkinliğinin düzenli olarak gözden geçirilmesi ve oluşabilecek değişiklikleri (teknoloji, iş amaçları ve süreçleri, tehditler, vb.) dikkate alarak, bilgi varlıklarının risk değerlendirmesinin belirli aralıklarla yeniden yapılmasını sağlar.

• Yerel BGYS Denetimleri, ilk taraf denetimleri olarak adlandırılan yönetim tarafından kapsamın uygun kalması ve süreçlerin iyileştirilmesini sağlamak için düzenli olarak kuruluş tarafından veya kuruluş adına danışman firmalar tarafından gerçekleştirilir.

BGYS'nin iyileştirilmesi için kurum tarafından önleyici ve düzeltici tedbirler alınması gereklidir. Olumsuzlukların yaşanmaması için, risk değerlendirme sonuçlarına bağlı olarak değişen riskler bazında önleyici tedbirler alınmalıdır. Gerçekleştirilen önleyici faaliyetler, olası sorunların yapacağı etkiye uygun olmalıdır. BGYS gereksinimleriyle olumsuzlukları gidermek üzere düzeltici önlemler alınmalıdır. Önleyici tedbirler için gerçekleştirilen faaliyetler çoğunlukla düzenleyici tedbirler için gerçekleştirilen faaliyetlerden daha az maliyetlidir.

ISO/IEC 27002, halen hazırlanma aşamasındadır. Bu standardın daha önceki bölümde açıklanan ISO/IEC 17799:2005 standardına eşdeğer olması beklenmektedir. Bilgi güvenliği ile ilgili standartların 27000 serisi altında yer almasından dolayı ISO/IEC tarafından böyle bir düzenlemeye gidilmiştir [21].

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. Geliştirilen standart içerisinde temel olarak; kritik başarı faktörleri, süreç yaklaşımı üzerine rehber, PUKÖ modeli rehberi, planlama süreç rehberi, uygulama süreç rehberi, kontrol süreç rehberi, önlem alma süreç rehberi ve diğer kurumlarla birlikte çalışma gibi konu başlıklarının yer alması beklenmektedir [22].

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 2008 yılı içerisinde yayınlanması beklenmektedir [23].

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 [24].
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 [25].

ISO/IEC 27007, ISO 27001 standardına göre BGYS denetlemesinde kullanılacak kılavuz niteliğinde geliştirilmesi düşünülen bu standart 2009 yılında tamamlanması beklenmektedir [26].

ISO/IEC 27031, standardı ISO 17799/27002 standardı esas alınarak telekom sektörü için özel olarak geliştirilmektedir. Kısa süre içerisinde ITU-T X.1051 ve ISO/IEC 27031 ismiyle yayınlanması beklenmektedir [27].

5.3. Türk Standartları (Turkish Standards)

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 süreklilik sağlayan, bilgi güvenliği yönetimi ile ilgili tavsiyeleri içermektedir.

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 standardı olarak kabul edildiğinden TS 17799–2 standardı TSE tarafından iptal edilmiştir [28].

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 standardın tercümesidir.

5.4. Belgelendirme (Certification)

BGYS'de belgelendirme, kurumsal bilgi güvenliğinin standartlara uyumlu bir şekilde yönetildiğine dair otoriteler tarafından verilen sertifikasyonlar aracılığıyla yapılmaktadır. Dünyada ve ülkemizde kurumsal bilgi güvenliği yönetim sistemlerinin belgelendirilmesinde uyumluluğa esas teşkil eden standart 2005 yılına kadar BS7799–2 standardı olurken bu yıldan sonra ISO/IEC 27001 standardı olarak değiştirilmiştir. 15 Nisan 2006 tarihine kadar olan 6 aylık bir hazırlık dönemi sırasında, denetimler ve belgelendirme ISO/IEC 27001:2005 veya BS 7799–2:2002 standartlarına göre gerçekleştirilmiştir. Ancak, bu süre içerisinde yayınlanmış olan yeni bir BS 7799–2:2002 sertifikasının, 15 Nisan 2007 tarihine kadar ISO/IEC 27001:2005'e geçişi tamamlanmıştır. 15 Nisan 2006 tarihinden sonra ise bütün denetimler ve belgelendirmeler ISO/IEC 27001:2005 standardına göre gerçekleştirilmiştir. ISO/IEC 27001:2005 belgelendirmesi için yapılması gereken altı aşama aşağıda kısaca açıklanmıştır [29].

Aşama 1: ISO/IEC 27001:2005 standardının tüm gereklerinin yerine getirilmesi ve standartta belirtilen yönetim iskelet yapısının oluşturulması.

Aşama 2: Uyumluluk denetimleri için yetkilendirilmiş sertifikalandırma kurumuna ön başvuru yapılır. Bu başvuruya istinaden denetimi yapacak firma belgelendirme için maliyet ve zaman çizelgesi sunar.

Aşama 3: Maliyet ve zaman çizelgesi kurum tarafından onaylanarak denetimi gerçekleştirecek firmaya resmi başvuru yapılır.

Aşama 4: Denetimi gerçekleştirecek olan kurum güvenlik politikasını, risk değerlendirmesi dokümanlarını, risk eylem planını, uygunluk beyanını (SOA) ve güvenlik prosedürlerini içeren dokümantasyonu gözden geçirir. Bu işlem sonucunda, bilgi güvenliği yönetim sistemindeki sorunlu olan ve çözüme kavuşturulması gereken herhangi bir zayıflığın veya göz ardı edilen bir hususun ortaya çıkarılması hedeflenir.

Aşama 5: Masaüstü kontrolü başarılı şekilde sonuçlandıktan sonra, denetim firmasının belirlediği denetçiler tarafından yerinde (on-site) denetim gerçekleştirilir. Kuruluşun büyüklüğüne ve iş tipine uygun kontrollerin olup olmadığı gözden geçirilir ve elde edilen sonuçlara göre kurumlara önerilerde bulunulur.

Aşama 6: Değerlendirmenin başarı ile tamamlanmasının ardından, Bilgi Güvenliği Yönetim Sisteminin kapsamını açık bir şekilde tanımlayan bir sertifika verilecektir. Bu sertifika 3 yıl boyunca geçerliliğini korur ve rutin değerlendirme ziyaretleri ile desteklenir.

ISO/IEC 27001 standardına göre kurulmuş olan bir bilgi güvenliği yönetim sistemi ile, kurumların bilgi güvenliği yönetiminde, kapsamlı prosedürler aracılığıyla güvenlik kontrollerini sürekli ve düzenli olarak işletmeyi ve sistemin sürekli iyileştirilmesi gerçekleştirilmektedir. Güven ve güvenilirliğin hayati önem taşıdığı alanlarda hizmet veren kuruluşların, uluslararası geçerlilikte bilgi güvenliği yönetim sistemleri standardına uygunluk belgesine sahip olması, hem mevzuat hem de kuruluşun güvenli işleyişi açısından bir zorunluluk olarak değerlendirilmektedir.

Kurumların ISO/IEC 27001 sertifikası almasının avantajları maddeler halinde aşağıda listelenmiştir [30].

- Kredilendirilebilirlik, güven ve itimat: Belgelendirme, kurum veya kuruluşun bilgi güvenliğini dikkate aldığını, bilgi güvenliğinin sağlanması için gerekli olan adımları uyguladığını ve kontrol ettiğini ispatlamaktadır. Bu sayede kurumlar veya kuruluşlar birlikte iş yaptıkları veya hizmet verdikleri kurum veya bireylerin tüm bilgilerinin BGYS sayesinde güvende tutulacağı konusunda verdikleri taahhütten dolayı iş yaptıkları kurum, kuruluş veya bireylerin kendilerini güvende hissetmelerini sağlayacaklardır. Belgelendirme sonucunda özellikle özel sektör firmalarında rekabet anlamında sertifika almamış rakiplerinin bir adım önüne geçerek avantaj sağlayacaklardır. Ayrıca günümüzde uluslararası yapılan işlerde ISO/IEC 27001:2005 şartı koşulmaktadır.
- Tasarruf: Oluşabilecek güvenlik ihlallerine karşı kontrollerin uygulanması ile maliyetler düşmektedir. Sadece bir bilgi güvenliği ihlalinin oluşturacağı zarar bile çoğu zaman çok büyük maddi kayıplara yol açabilir. Belgelendirme işlemi kurumların maruz kalacağı bu tür ihlalleri azaltarak bilgi güvenliği ihlallerinden doğan zararları en aza indirecektir.
- Yasal Uygunluk: Belgelendirme işlemi, kanun ve tüzüklere uygunluğun yetkili ve ilgili makamlara yasal anlamda uygunluğun sağlandığına dair kanıt teşkil edilmesine yardımcı olur.
- Taahhüt: Belgelendirme işlemi, organizasyonun tüm aşamalarında taahhüt/bağlılığın sağlanması ve kanıtlanmasında yardımcı olur.
- Operasyonel Seviye Risk Yönetimi: Kuruluş genelinde, bilgi sistemleri ve zayıflıklarının nasıl korunacağı konusundaki farkındalık artar. Ayrıca donanım ve veriye daha güvenli bir şekilde erişim sağlanır.
- Çalışanlar: Çalışanların kuruluş içerisindeki sorumlulukları ve bilgi güvenliği konularındaki bilinçlerinin artmasını sağlar.
- Sürekli İyileşme: Düzenli olarak gerçekleştirilen denetimlere bağlı olarak bilgi sistemlerinin etkinliği izlenecek ve izleme sonucunda tespit edilen problemler giderilerek bilgi sistemlerinde genel anlamda bir iyileşme sağlanabilecektir.
- Onay: Organizasyon için tüm seviyelerde bilgi güvenliği varlığının bağımsız kuruluşlar tarafından onaylandığını göstermektedir.

6. GÜNCEL TEHDİTLER VE BULGULAR (RECENT THREATS AND FINDINGS)

Daha önceki bölümlerde de açıklandığı gibi günümüzde kurum ve kuruluşlar bilgilerini elektronik ortamlara açtıkça, elektronik ortamlarda yapılan iş ve işlemler artmakta karşılaşılan güncel tehdit ve tehlikelerde de doğal olarak artışlar gözlenmektedir. Zafiyet ve zayıflık açısından değerlendirildiğinde korunmasızlık seviyesinin yüksek olması nedeniyle güncel gelişmelerin en fazla yaşandığı alan web uygulamalarıdır. Günümüzde web uygulamaları, güncel bilgiye kurum, kuruluş veya bireylerin kolayca erişebilmesi için en kolay ve en etkin yöntem olarak karşımıza çıkmaktadır. Web üzerinden verilen hizmetler çoğaldıkça web'e yönelik saldırılar da her geçen gün artmaktadır. Bunun nedeni, web uygulamaları güvenliğinin ilgisizlikten ve bilgisizlikten kaynaklanan sebeplerden ötürü yeterince ciddiye alınmaması ve güvenli yazılım geliştirme tekniklerinin kullanılmaması olarak açıklanabilir.

Günümüzde web uygulama 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 [31]. 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) [32]. Web uygulama güvenliği konusunda dünyada kabul görmüş OWASP ve WASC tarafından belirlenen, web uygulamalarında en fazla rastlanan saldırılar bu bölümde anlatılacak olan güncel tehditler ve gelişmelere esas teşkil etmiştir.

6.1. Kimlik Doğrulama (Authentication)

Web uygulamalarında kimlik doğrulama mekanizmasını atlatmak veya istismar etmek için kullanılabilecek tehditlerdir. Kimlik doğrulamasında "sahip olunan bir nesne", "bilinen bir bilgi" veya "sahip olunan bir özellik" kullanılmaktadır [33]. Kimlik doğrulama saldırıları, web sitesinin kullanıcı, servis veya uygulama kimliğini doğrulayan sistemleri hedef alan tehditleri kapsar. Web sitelerinin, kimlik doğrulama mekanizmasını atlatmak veya istismar etmede kullanılan saldırı teknikleri, kaba kuvvet,

yetersiz kimlik doğrulamaları ve şifre kurtarma denetimlerinin zayıflığının istismar edilmesi olarak sıralanabilir [34].

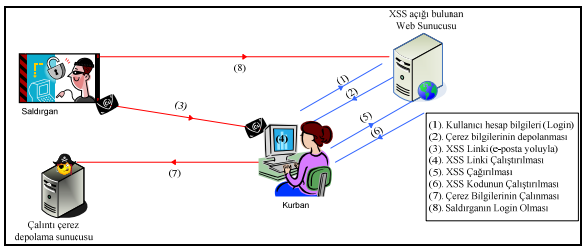
6.2. Yetkilendirme Zafiyeti (Authorization Vulnerability)

Yetkilendirme zafiyetleri, bir web sitesinin kullanıcı, servis veya uygulamanın istenen bir işlemi gerçekleştirmesi için gereken izinleri belirlemek için kullanılan yöntemlerin istismar edilmesini hedef alan saldırılardan etkilenmektedir. Yetkilendirme tehditlerini, oturum bilgisi tahmin etme, yetersiz yetkilendirme, yetersiz oturum sonlandırma, oturum sabitleme olmak üzere farklı gruplarda sınıflandırmak mümkündür.

6.3. Siteler Arası Kod Yazma (Cross Site Script)

Siteler arası kod yazma yöntemiyle yapılan saldırılar, 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. XSS yöntemiyle yazılan küçük kodlar, HTML kodları arasına enjekte edildiğinden bazı kaynaklarda bu yöntemin adı HTML kod enjeksiyonu olarak adlandırılmaktadır. XSS kodları genellikle HTML/JavaScript dilinde yazılmaktadır ancak VBScript, ActiveX, Java, Flash veya web tarayıcılar tarafından desteklenen diğer dillerde de kodlama yapılabilmektedir [35].

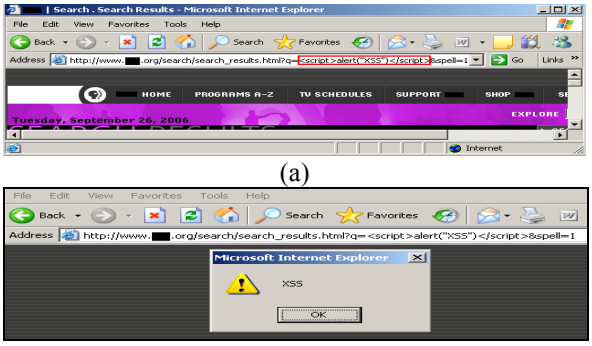
XSS yöntemiyle zararlı kodun kullanıcı web tarayıcısında çalıştığında, zararlı kod sunucu web sitesinin tarayıcı için tanımlı olduğu güvenlik ayarları kapsamında çalışacaktır. Eğer web tarayıcısı üzerinde herhangi bir kısıtlamaya gidilmemişse zararlı kod vasıtasıyla tarayıcı tarafından erişilen her türlü hassas veri okunabilir, değiştirilebilir ve e-posta aracılığıyla farklı yerlere iletilebilir. XSS yöntemiyle kullanıcı bilgisayarı üzerindeki oturum çerezleri çalınabilir, kullanıcının web tarayıcısı başka bir adrese yönlendirilebilir, web siteleri üzerinde bilgi toplama amaçlı kodlar çalıştırılabilir, sazan avlama yöntemine davetiye çıkartılır, web sayfalarının değiştirilmesi veya hizmet aksattırma saldırılarının yapılmasını sağlamaktadır. XSS saldırı yöntemi şematik gösterimi Şekil 6'da verilmiştir.



Şekil 6. XSS yönteminin mantıksal gösterimi

Şekil 6'da görüldüğü gibi XSS yönteminde (1) nolu adımda kullanıcının şifre ve parolasını kullanarak web uygulamasına giriş yapması sonucunda (1), kullanıcıya ait hesap bilgileri çerez formatında kullanıcı bilgisayarında saklanmak üzere XSS açığı bulunan uygulama sunucu bilgisayarından kullanıcı bilgisayarına gönderilmektedir (2). Saldırgan XSS zafiyetini kullanan URL (Uniform Resource Locator)'yi sazan e-posta aracılığıyla kurbana göndererek (3), XSS açığı bulunan web sunucusuna gitmesini sağlayacak bağlantıya tıklamasını sağlar (4). XSS açığının bulunduğu sayfanın çağırılmasıyla (5), XSS saldırısı yapılmasını sağlayacak kod çalıştırılır (6). XSS kodunun çalıştırılmasıyla kullanıcı bilgisayarında daha önceden depolanan çerez bilgileri çalınarak saldırganın denetiminde olan sunucu bilgisayarına depolanır (7). Çalıntı çerez depolama sunucusundaki kullanıcı erişim bilgilerinin yer aldığı çerez saldırgan tarafından kullanılarak web uygulamasına kurbanın kullanıcı haklarıyla erişir (8). XSS yöntemleri kalıcı, geçici ve DOM (Document Object Model) temelli olmak üzere üç farklı kategoride sınıflandırılmaktadır [36].

Kalıcı olmayan XSS yöntemi, kullanıcının zararlı kod içeren özel olarak değiştirilmiş linkleri ziyaret etmesini gerektirir. Link ziyaret edildiğinde, URL içine gömülü zararlı kod, istemci tarafına gönderilir ve kod kullanıcının web tarayıcısında çalışır. Kalıcı olmayan XSS yöntemiyle ilgili örnek Şekil 7'de gösterilmiştir.



(a)

(b)

Şekil 7. Kalıcı olmayan XSS kodu işlemleri a) Kodlama, (b)İcra ettirme

Şekil 7(a)'da XSS açığı bulunan bir web sitesinde arama yapılmasını sağlayan HTML kodları arasına yerleştirilen XSS kodu web tarayıcısının adres kısmında kırmızı dikdörtgen içerisinde gösterilmektedir. Bu şekilde hazırlanan linkin kullanıcılar tarafından ziyaret edilmesi sağlandığında XSS yöntemiyle sızma testi Şekil 7(b)'de gösterildiği gibi başarıyla gerçekleştirilmiş olacaktır.

Kalıcı XSS saldırısı, mesaj panoları, ziyaretçi defterleri, tartışma forumları, web posta mesajları gibi kullanıcı tarafından web sitelerine girdi yapılabilecek hedefler seçilerek zararlı kodların sunucu tarafında XML dosyaları veya veri tabanlarında depolanmasıyla sağlanır. Bu sızma yönteminde kullanıcının herhangi

bir linke tıklamasına gerek yoktur, sadece zararlı kodu içeren web sayfasının tarayıcıda çalışması yeterlidir. Kalıcı XSS yöntemiyle zararlı kod hedef web sitesine sızdırıldıktan sonra; hedef web sitesini ziyaret eden geniş bir kullanıcı kitlesi bu durumdan etkilenmektedir.

DOM temelli XSS yönteminde, dinamik web sayfaları üzerinde çalışan diğer XSS yöntemlerinden farklı olarak sunucu tarafına zararlı kod gönderilmesine ihtiyaç duyulmayan, kullanıcı tarafında çalıştırılan kod parçalarını içerir [37]. Bu yöntemle yapılan saldırılarda kullanıcının web tarayıcısında etkili olacak DOM nesneleri kullanılmaktadır.

6.4. Komut Çalıştırma (Command Execution)

Komut çalıştırma yöntemi, web uygulamalarında uzaktan çalıştırılan komutlar yardımıyla yapılan saldırılardır. 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.

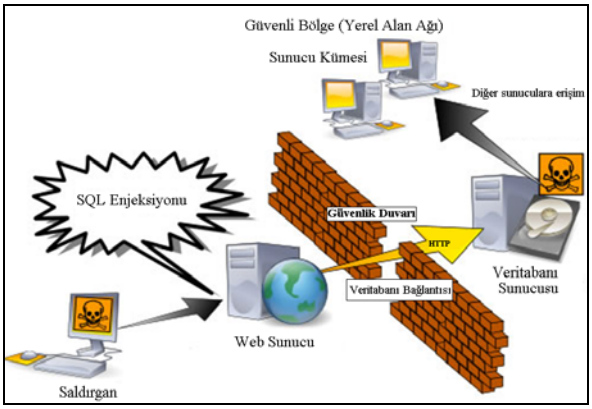
6.5. SQL Enjeksiyonu (SQL Injection)

SQL veritabanları, sorgu yapmak üzerine özelleşmiş hem ANSI hem de ISO standardı olan yapısal bir programlama dilidir. Değişen büyüklükteki ilişkisel veritabanı uygulamalarına SQL sorguları aracılığıyla ulaşılabilir. SQL'i destekleyen birçok veritabanı ürünü (Oracle, MS SQL Server, MS Access, Ingres, DB2, Sybase, Informix, vb) standart dile özel eklentiler getirir [38]. Web uygulamaları kullanıcı kaynaklı girdileri, dinamik web sayfası talepleri için, değişik SQL cümleleri oluşturmada kullanabilir.
SQL enjeksiyonu yöntemi, kullanıcı girdilerine göre SQL cümleleri oluşturan web sitelerinde, kullanıcı kaynaklı girdilerin doğrulanmaması veya yetersiz doğrulanmasından kaynaklanan zafiyetlerin kullanılarak, SQL cümlelerinin manipüle edilmesini sağlayan sızma testleridir [39]. SQL enjeksiyonu sızma yöntemiyle yapılabilecek işlemler aşağıda sıralanmıştır.

- Veri tabanları üzerinde istenmeyen işlemler (sorgulama, ekleme, silme, değiştirme, vb.) yapılabilir.
- Kimlik doğrulama mekanizmaları atlatılabilir.
- İşletim sistemi seviyesinde komutlar çalıştırılabilir.
- Etki alanında yeni kullanıcılar veya gruplar oluşturulabilir.

Eğer bir web uygulaması, kullanıcı kaynaklı girdiyi etkin bir biçimde denetlemezse, SQL enjeksiyon yöntemiyle arka taraftaki SQL cümlesi oluşumu değiştirilerek güvenlik ihlalleri oluşturulabilir. SQL enjeksiyon yöntemiyle SQL cümlesi değiştirilerek bilgisayar sistemlerine sızılması durumunda, SQL servisini çalıştıran kullanıcı haklarına sahip olunacaktır. Veritabanı üzerinde bu haklara sahip olan kişi ileri derece sızma teknikleri kullanarak veritabanı dışındaki diğer sunucu bilgisayarları üzerinde de erişim hakkı kazanabilir.

Şekil 8'de şematik olarak gösterildiği gibi saldırgan hedef web sitesi üzerinde SQL enjeksiyonu yapabileceği dinamik içerikli web sayfalarını tespit ettikten sonra, SQL enjeksiyonu aracılığıyla veritabanı sunucu bilgisayarına veritabanını çalıştıran servisin (muhtemelen üst seviyede erişim hakları bulunan yönetici hesapları) kullanıcı hesabıyla ulaşabilir. Veritabanı sunucu bilgisayarı üzerinde, SQL enjeksiyonu yardımıyla işletim sistemi seviyesinde komutlar çalıştıran saldırganın bir sonraki hedefi diğer bilgisayarlar ve özellikle sunucular olacaktır. Saldırgan, diğer sunucu bilgisayarlarına veritabanı kullanıcı hesabıyla bağlantı yaptıktan sonra tüm sunucu bilgisayarlara daha sonra doğrudan bağlanabilmesi (remote desktop, telnet, http, ftp, vb.) için gerekli olan servisleri kendi kullanımına açabilecek ve saldırıdan beklediği sonuçları elde edebilecektir.



Şekil 8.SQL Enjeksiyonu şematik gösterimi

Güncel tehditler incelendiğinde bilgi güvenliği alanında yaşanan güvenlik ihlallerinin, ağ ve sistemlerden web uygulamalarına doğru hızlı bir şekilde kaydığı bu çalışmada elde edilen önemli bulgulardandır. Bu çalışmada elde edilen bir diğer bulgu ise literatürde de vurgulandığı gibi ülkemizde de en fazla güvenlik açıklarına 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

dâhil olduğu büyük bir çoğunluk tarafından anlaşılamadığı, bilinmediği veya bilinse dahi uygulanamadığı da görülmektedir.

Kurumsal bilgi güvenliğinin sağlanmasıyla ilgili olarak bu çalışmada güvenliğin bir ürün veya hizmet olmadığı, insan faktörü, teknoloji ve eğitim üçgeninde güvenlik standartlarına bağlı olarak yaşayan canlı bir süreç olduğu ve bu üç unsur arasında tamamlayıcılık olmadığı sürece yüksek seviyede bir güvenlikten bahsedebilmenin mümkün olamayacağı da saptanmıştır.

7. SONUÇLAR VE DEĞERLENDİRMELER (RESULTS AND CONCLUSIONS)

Bu çalışmada, kurumsal bilgi güvenliğinin sağlanmasında önemli olan unsurlar gözden geçirilmiştir. Yüksek seviyede KBG sağlanabilmesi için bilgi güvenliği standartlarının bilinmesi ve uygulanmasının yanında güncel tehditlerin bilinmesi önemlidir. Bu tehditlerin tespit edilebilmesi ve ortadan kaldırılabilmesi için mevcut bilgi varlıklarının belirli aralıklarla sızma testlerine tabii tutulması zafiyet ve açıkların giderilmesi açısından önemlidir. Yüksek seviyede bir KBG sağlanabilmesi için teknoloji-insan-eğitim üçgeninde yönetilen bir yaklaşımın dikkate alınması gerektiği tespit edilmiştir. Yapılan diğer tespitler aşağıda sunulmuştur.

- 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" 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, uygulamaları 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 bünyelerinde güvenlik uzmanları çalıştırmaları veya danışmanlık hizmetleri almaları gerekmektedir. BGYS uygulamaları, kurumlar tarafından başarılı bir şekilde uygulandıktan sonra kuruluşların bilgi güvenliğini yönettiklerine dair uluslararası alanda geçerli sertifikasyona sahip olmaları önemlidir.
- Bilgi güvenliğinin yönetilmesi bilgi güvenliğinin sağlandığı anlamına gelmemektedir. BGYS'nin kurumsal bilgi güvenliğini taahhüt ettiği seviyede sağlayıp sağlamadığı, sağlamıyorsa eksikliklerinin neler olduğu, güvenlik denetimlerinin güvenli biçimde kurulup kurulmadığı, güvenlik denetimlerinin etkin ve politikalara uygun olarak uygulanıp uygulanmadığı, iyi bir belgelendirme yapılıp yapılmadığı gibi bilgi güvenliğinin sağlanması açısından çok kritik olan soruları cevaplamanın tek yolu BGYS kapsamında belirlenen bilgi varlıklarının (insan faktörü, yazılımlar, donanımlar, ortamlar, vb.) güvenliğini "sızma testleriyle" test etmekten geçmektedir.

Kurumsal bilgi güvenliğinin yüksek seviyede sağlanmasında sızma testlerinin katkısı çok yüksektir. Sızma testleri felaket başa gelmeden önce, onu önleyecek ve ona karşı savunulacak ihtiyaçların ve tedbirlerin alınmasında kullanılan önemli bir erken uyarı sistemidir. Bu önemden dolayı, sızma testleri belirli periyotlarda (bu yılda en az 2-3 kez olabilir) veya sistem yenilenmelerinde yapılmalı ve kurumsal bilgi güvenliğinin yüksek seviyede sağlanmasındaki rolü her zaman dikkate alınmalıdır.

Yukarıda anlatılan hususların yanında, yüksek seviyede kurumsal bilgi güvenliğinin sağlanmasında aşağıdaki hususlara da dikkat edilmesi önerilmektedir. Bunlar:

- Kurumsal bilgi güvenliğini sağlamanın dinamik bir süreç olduğu ve süreklilik arz ettiği,
- Kurumsal bilgi güvenliğinin sadece teknolojiyle sağlanır yaklaşımından uzaklaşılarak insan-eğitim-teknoloji üçgeninde yeni bir yaklaşımla sağlanması gerektiği,
- Uluslararası standartlara uygun olarak yapılması ve uygulanması gerektiği,
- Standartlar yüksek seviyede bir güvenliği garanti etse de bazen standartlarında yetersiz kalabileceği,
- Kurumsal bilgi güvenliği seviyesinin güncel durumunun belirlenmesi amacıyla iç ve dış ortamlardan zaman zaman bağımsız uzman kuruluşlar tarafından denetlenmesi gerektiği,
- Kurumsal bilgi güvenliğinin yönetilmesinin zorunlu bir süreç olduğu ve her zaman iyileştirmelere ihtiyaç duyulduğu ve
- En zayıf halka kadar güvende olunacağı varsayımıyla hareket edilerek gerekli önlemlerin alınması gerektiği

bilinmeli ve uygulanmalıdır.

KAYNAKLAR (REFERENCES)

1. Barrett, N., "Penetration testing and social engineering: Hacking the weakest link", **Information Security Technical Report**, 8(4):56-58, 2003.
2. Arce, I., "The weakest link revisited" **IEEE Security & Privacy Magazine**, 1(2):72-74, 2003.
3. İnternet: Computer Incident Advisory Capability "PDF XSS Vulnerability"

http://www.ciac.org/ciac/bulletins/r-096.shtml, 07.07.2007.
4. Dodge, C. R., Carver, C., Ferguson, J. A., "Phishing for user security awareness" **Computers & Security**, 26(1): 73, 2007.
5. İnternet: Netcraft "Phishing By The Numbers: 609,000 Blocked Sites in 2006" http://news.netcraft.com/archives/2007/01/15/phishing_by_the_numbers_609000_blocked_sites_in_2006.html, 07.07.2007.
6. İnternet: Message Labs "2006: The Year Spam Raised Its Game and Threats Got Personal" http://www.messagelabs.com/portal/server.pt/gateway/PTARGS_0_5885_404_443_670_43/http%3B/0120-0176-CT01/publishedcontent/publish/about_us_dotcom_en / news events/press_releases/DA_174397.html, 07.07.2007.
7. Kudat, B., "Kötü adamların hızına yetişen daha güvenli", **BThaber**, 604:15, 2007.
8. Vural, Y., "Kurumsal Bilgi Güvenliği ve Sızma Testleri" Yüksek Lisans Tezi, **Gazi Üniversitesi Fen Bilimleri Enstitüsü**, 40, 2007.
9. İnternet: Wikipedia, "ISO/IEC 27001", http://en.wikipedia.org/wiki/ISO_27001, 07.08.2007.
10. Thow-Chang, L., Siew-Mun, K., and Foo, A., "Information Security Management Systems and Standards" **Synthesis Journal**, 2(2):5,8, 2001.
11. Kalman, S., "Web Security Field Guide", **Cisco Press**, Indianapolis, sf.36, 37, 2003.
12. İnternet: Wikipedia "BS-7799" http://en.wikipedia.org/wiki/BS_7799, 08.07.2007.
13. Osborne, M., "How to Cheat at Managing Information Security", **Syngress Publishing Inc.**, Rockland, 90, 2006.
14. British Standards Institute, "Information Technology — Security Techniques — Code of Practice for Information Security Management", **BSI BS 7799-1:2005,** Bristol **,** 4,5,7,9,19,23,29,37 2005.
15. İnternet: BSI "Information Security Management Systems Guidelines for Information Security Risk Management" http://www.bsi-global.com/en/Shop/PublicationDetail/?pid=000000000030125022&recid=2557, 08.07.2007.
16. İnternet: International Organization for Standardization-ISO "JTC 1 / SC 27" http://www.iso.org/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeDetailPage.TechnicalCommitteeDetail?COMMID=143, 09.07.2007.
17. Saint-Germain, R., "Information Security Management Best Practice Based on ISO/IEC 17799", **The Information Management Journal**, 39:61-62, 2005.
18. İnternet: BSI Eurasia "ISO/IEC 17799:2005 Nedir?" http://www.bsi-turkey.com/BilgiGuvenligi/Genel-bakis/BS7799nedir.xalter, 09.07.2007.
19. İnternet: Wikipedia "ISO 27000 Series" http://en.wikipedia.org/wiki/ISO_17799, 08.07.2007.
20. Türk Standardları Enstitüsü, "Bilgi Teknolojisi– Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri-Gereksinimler", **TSE- TS ISO/IEC 27001,** Ankara, 3-13, 2006.
21. İnternet: ISO 27001 Security "ISO/IEC-17799&ISO/IEC-27002" http://www.iso27001security.com/html/iso17799.html, 09.07.2007.
22. İnternet: ISO 27001 Security "ISO/IEC 27003" http://www.iso27001security.com/html/iso27003.html , 09.07.2007.
23. İnternet: ISO 27001 Security "ISO/IEC 27004" http://www.iso27001security.com/html/iso27004.html (09.07.2007).
24. İnternet: ISO 27001 Security "ISO/IEC 27005" http://www.iso27001security.com/html/iso27005.html, 09.07.2007.
25. İnternet: ISO 27001 Security "ISO/IEC 27006" http://www.iso27001security.com/html/iso27006.html, 09.07.2007.
26. İnternet: ISO 27001 Security "ISO/IEC 27007" http://www.iso27001security.com/html/iso27007.html, 09.07.2007.
27. İnternet: ISO 27001 Security "ISO/IEC 27031" http://www.iso27001security.com/html/iso27031.html, 09.07.2007.
28. Türkiye Bilişim Derneği, "E-Devlet Uygulamalarında Güvenlik ve Güvenilirlik Yaklaşımları 4. Çalışma Grubu Sonuç Raporu**", TBD Kamu-BİB IV, Ankara,** 9, 11, 17, 2005.
29. İnternet: BSI Eurasia "BSI Belgelendirme Yöntemi" http://www.bsi-turkey.com/BilgiGuvenligi/ISMStescil/BSItescilyontemi.xalter?print_only=1, 24.01.2008.
30. İnternet: BSI Eurasia "Bilgi Güvenliği Yönetim Sisteminin Belgelendirilmesi" http://www.bsi-turkey.com/BilgiGuvenligi/ISMStescil/index.xalter, 24.01.2008.
31. İnternet: OWASP "About The Open Web Application Security Project" http://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project, 24.01.2008.
32. İnternet: Web Application Security Consortium "About Us" http://www.webappsec.org/aboutus.shtml , 24.01.2008.
33. Hansche, S., "Official (ISC2) Guide to the CISSP Exam", Auerbach Publications, New York, 12, 2003.
34. İnternet: Web Application Security Consortium "Weak Password Recovery Validation" http://www.webappsec.org/projects/threat/classes/weak_password_recovery_validation.shtml 24.01.2008.

35. İnternet: Web Application Security Consortium "Cross-site Scripting" http://www.webappsec.org/projects/threat/classes/cross-site_scripting.shtml, 24.01.2008.
36. İnternet: Amit Klein "DOM Based Cross Site Scripting or XSS of the Third Kind" http://www.webappsec.org/projects/articles/071105.shtml, 24.01.2008.
37. İnternet: The World Wide Web Consortium (W3C) "Document Object Model FAQ" http://www.w3.org/DOM/faq.html#what, 24.01.2008.
38. Chapela, V., "Advanced SQL Injection" http://www.owasp.org/images/7/74/Advanced_SQL_Injection.ppt, 24.01.2008.
39. Anley, C., "Advanced SQL Injection In SQL Server Applications", Next Generation Security Software Publication, Surrey, 18- 21, 2002.