E-Devlet Kapısı Projesi Bilgi Güvenliği ve Risk Yönetimi: Türkiye Uygulaması

Erhan KUMAŞ[1], Burak BİRGÖREN[2]

Türk Telekomünikasyon A.Ş. Genel Müdürlüğü, Bilgi Teknolojileri Direktörlüğü, F Blok, Aydınlıkevler, ANKARA[1]
Endüstri Mühendisliği Bölümü, Mühendislik Fakültesi, Kırıkkale Üniversitesi[2]

Özet— İçerisinde bulunduğumuz yüzyılın toplumsal yapısını ve yaşam tarzını etkileyen en önemli faktörlerden birisi, "Bilgi ve İletişim Teknolojileri" olmuştur. BİT alanındaki gelişim; bilginin üretilmesi, saklanması, düzenlenmesi, işlenmesi, taşınması, hizmete sunulması ve kullanılmasında büyük bir değişimi beraberinde getirmiştir. Bu alandaki hızlı değişim, ülkelerin geleceğe yönelik politikalarını da etkilemiş; bilgi ve iletişim teknolojileri alt yapısının geliştirilmesi ve bunların yaygın kullanımının teşvik edilmesi, pek çok ülkenin öncelikleri arasına girmiştir. Bilgi ve iletişim teknolojileri alanında dünyadaki gelişmelere paralel olarak, özellikle e-devlet konusunda Türkiye'de de stratejiler üretilmiş ve bu stratejilere uygun projeler geliştirilmiştir.

Elektronik ortamda sunulan hizmetlere olan talebi en çok etkileyen faktörlerden biri güvenliktir. Özellikle üçüncü ve daha ileri düzeylerde, kişisel bilgilerin kullanımı ve ödemeleri de içerecek şekilde sunulan elektronik hizmetlerde, güvenlik büyük önem taşımaktadır. Bu alandaki bir zafiyet, bütün e-Devlet hizmetlerini olumsuz etkileyip, talep azalmasına yol açma riski taşımaktadır. Bu makalede; e-Devlet Kapısı Projesi çerçevesinde yapılmış olan bilgi güvenliği altyapısını kapsayan bir risk analizi çalışması yapılmış ve elde edilen sonuçlar paylaşılmıştır.

Anahtar kelimeler— Bilgi Güvenliği Yönetimi, e-Devlet Kapısı Projesi, Risk Yönetimi

E-Government Gateway Project, Information Security and Risk Management: Turkish Case

Abstract— One of the most important factors that influences current century's social structure and life style is "Information and Communication Technologies". This technological development leads changes in producing, keeping, editing, manipulating, carrying, serving and using information. The rapid change in science and technology has also influenced future politics of states; developing substructures of information and communication technologies and promoting common use of technologies have become major priorities for many states. In parallel with the development all around the world in information and communication technologies, many strategies and many projects along with these strategies were produced in Turkey, especially in e-state issues.

The most effective factor influencing demand to electronical services is security. Particularly in third and other advanced levels, in usage of personal information and electronical services including paying; security is very important. Any weakness in that issue will affect negatively all e-state services, and carry a risk causing decline in demand. In this article, a risk analysis including information security infrastructure within the framework of e-State Gate project is carried out and the results of the analysis are shared.

Keywords— Information Security Management, e-Government Gateway Project, Risk Management

1. GİRİŞ

Küreselleşme olgusunun gelişiminde önemli etkisi olan bilgi ve iletişim teknolojilerindeki yenilikler, ekonomik ve sosyal yaşamın her alanını ve toplumun tüm kesimlerini çeşitli yönlerden etkisi altına almakta; kamu yönetimi yaklaşımlarını, iş dünyasının iş yapma usullerini ve bireylerin yaşamlarını derinden etkilemekte, bir başka ifadeyle toplumsal bir dönüşüme neden olmaktadır. 21. yüzyıla damgasını vuran bu teknolojiler, yeni bir toplumsal dönüşüme yani "bilgi toplumu"na da zemin oluşturmaktadır [1].

Bilgi ve iletişim teknolojilerinde son yıllarda gözlenen gelişmeler, kamu yönetiminde yapısal bir dönüşüm ihtiyacını da gündeme getirmiştir. Kamu hizmetlerinin

elektronik ortamda sunulması anlamına gelen e-devlet sayesinde halkın hizmete erişimi daha hızlı ve daha ucuz olması beklenmektedir. Ancak, e-devlet olanaklarından azami ölçüde yararlanılması, kamu iş süreçlerinin vatandaşın bakış açısı ile yeniden tasarlanmasını ve kamu kurumlarının birlikte daha etkin ve verimli çalışabilirliğinin sağlanmasını gerektirmektedir [2].

E-Devlet Kapısı Projesi organizasyonunda bulunan ve projenin tüm kamu kurumlarında benimsenmesi ve uygulanabilmesi amacıyla kurulması öngörülen alt komisyonlar bulunmaktadır. Bunlardan "Güvenlik Grubu" nun üstlendiği görev ve sorumluluk önem arz etmektedir. E-Devlet Kapısında güvenlik bütün platforma yayılacak bir katman olacaktır. Güvenlik Grubu güvenlik katmanının tutarlı ve bütün platform için geçerli politikalarını, uygulama esaslarını belirleyen ve spesifik sistemlerden sorumlu personellerle birlikte uygulayan ekip olması hedeflenmektedir. Bu bağlamda kamu kurumlarından resmi yollar ile bildirilen kurum temsilcileri, bulundukları kurumların güvenlik liderleri olacak şekilde eğitilmeleri konusunda gerekli yönlendirmelerin yapılması gerekmektedir. Yapılacak olan yönlendirmeleri genel olarak sıralayacak olursak;

- Bilgi güvenliği ekibinin kurulması (Güvenlik lideri + Birimlerin temsilcileri),
- Bilgi güvenliği ekibinin eğitilmesi,
- Kapsamın belirlenmesi,
- Danışman seçilmesi veya önderlik edilmesi süreci,
- Pilot bir birim seçilerek şablonların oluşturulması,
- Dokümantasyon çalışmaları ve belgelendirme sürecinin tamamlanması,

şeklindedir. Bu noktada yukarıda belirtilen adımlar bir projenin, kurumun ve/veya şirketin bilgi güvenliği ve risk yönetimi kavramı açısından kurgulanması sürecinde takip edilebilir aşamalardır.

Avrupa Komisyonu tarafından Avrupa için Sayısal Gündem (Digital Agenda for Europe) başlıklı strateji 19/05/2010 tarihinde yayımlanmıştır. Hızlı internet erişimine ve birlikte çalışabilir uygulamalara dayanan ortak pazarın ekonomik ve sosyal fayda üretmesini hedefleyen Sayısal Gündemin 7 temel başlığından bir tanesinin "Güvenlik" olması manidardır. Doküman içerisinde; AB bünyesindeki ülkelerde yapılan araştırmada; internet kullanan vatandaşlar arasında yapılan incelemelerde web kullanıcılarının sadece %12'sinin çevrimiçi işlem yapma konusunda güvenlik endişesinin olmadığı ortaya çıkmıştır. E-Dönüşüm çabaları ile ilgili olarak sistemlerdeki açıklıkların, zaafiyetlerin oluşturduğu tehdit ve risklerin; güvenlik ile ilgili sektörü canlandıracağı tespiti yapılmaktadır. Sayısal Gündem dokümanı ve eylem planı ile birlikte AB bünyesinde oluşabilecek siber saldırılara karşın kişisel verilerin korunması ile ilgili önlemler alınması hedeflenmiştir. [3]

Bu çalışmada, e-Devlet Kapısı Projesi çerçevesinde yapılmış olan ve bilgi güvenliği altyapısını kapsayan risk analizi çalışması neticesinde elde edilen sonuçların değerlendirilmesi hedeflenmektedir.

2. TÜRKİYE'DE E-DEVLET KAPISI PROJESİ RİSK YÖNETİMİ SÜRECİ

Bir kuruluşu risk ile ilgili olarak kontrol etmek ve yönlendirmek amacıyla kullanılan koordineli faaliyetler bütününe risk yönetimi denilmektedir [4]. Bilgi ve iletişim sistemlerinde risk yönetimi teknikleri tüm bilgi sistemine, bu sistemi oluşturan ayrı sistem parçalarına ya da servislere uygulanabilir. Risk yönetiminin amacı, kurumun bilgi varlıkları için, uygun bir seviyede korunmanın sağlanmasıdır. "E-Devlet Kapısı Projesi" çerçevesinde uygulamaya alınan risk değerlendirme sürecinin detayları makale'nin ilerleyen bölümlerde derinlemesine irdelenecektir.

2.1. Risk Analizi

ISO/IEC 27001:2005 standardında; kaynakları belirlemek ve riski tahmin etmek amacıyla bilginin sistematik kullanımı olarak tanımlanmaktadır. Tespit edilmiş veya edilecek olan riskler ile ilgili tehditlere ilişkin gerçekleşme olasılıkları ve tehditlerin gerçekleşmesi durumunda ortaya çıkabilecek olumsuz sonuçlara ilişkin düzeyler e-devlet kapısı projesinde Çizelge-1'deki skala baz alınarak belirlenmiştir:

Çizelge 1. Olasılık skalası

Düzey	Olasılık
5	Neredeyse her seferinde gerçekleşir
4	Sıklıkla meydana gelebilir
3	Bazen meydana gelebilir
2	Meydana gelmesi çok olası değildir ama yine de olabilir
1	Çok nadiren meydana gelebilir

Çizelge-1'de tanımlanmış skala yardımıyla tehditlerin gerçekleşme olasılıkları ve potansiyel sonuçları belirlendikten sonra olasılık ve sonuç değerleri ışığında Çizelge-2'deki matris kullanılarak risk düzeyleri hesaplanır.

2.2. Maliyet-Etkinlik Değerlendirmesi

Çizelge 2'de verilmiş olan risk düzey matrisi; yapılan analiz çalışması neticesinde belirlenen risklerin düşük, orta, yüksek ve çok yüksek düzeyde olma olasılıklarına göre nasıl tanzim edilmeleri gerektiği ile ilgili yardımcı olacaktır.

Çizelge 2. Risk düzeyi matrisi

		Potansiyel Sonuç Düzeyi				
		Önemsiz(1)	Az önemli (2)	Önemli(3)	Çok önemli (4)	Feci(5)
Olasılık	5	Orta (O)	Yüksek (Y)	Yüksek (Y)	Çok Yüksek (ÇY)	Çok Yüksek (ÇY)
	4	Orta (O)	Orta (O)	Yüksek (Y)	Yüksek (Y)	Çok Yüksek (ÇY)
	3	Düşük (D)	Orta (O)	Yüksek (Y)	Yüksek (Y)	Yüksek (Y)
	2	Düşük (D)	Düşük (D)	Orta (O)	Orta (O)	Yüksek (Y)
	1	Düşük (D)	Düşük (D)	Orta (O)	Orta (O)	Yüksek (Y)

e-Devlet Kapısı Projesi bünyesinde yapılan risk analizi çalışmasında Çizelge-1 ve Çizelge-2'de belirtilen kriterler ışığında irdelendiğinde tespit edilmiş olan toplam 434 risk'ten 61 tanesi "yüksek", 255 tanesi "orta" ve 118 tanesi "düşük" risk düzeyinde olduğu tespit edilmiştir. Bu durum Şekil-1'de görülebilmektedir.

Şekil 1. Adet ve risk düzeyi ilişkisi

Yukarıda anılan sayısal değerlerin nasıl tespit edildiği ilerleyen bölümlerde adım adım aktarılmaktadır. Bu bölümde hızlıca değinildiği taktirde;

- E-Devlet Kapısı Projesinin kapsamı belirlenmiştir,
- Proje ile ilgili "Bilgi Güvenliği" ekibi kurulmuştur,
- Projenin bütün varlıklarına ilişkin bir envanter üretilmiştir, (Çizelge 4)
- Üretilen bu varlık envanteri üzerinde tehdit tanımlaması yapılmıştır,
- Bu tehditlerle ilgili proje bünyesindeki zafiyetler / açıklıklar tanımlanmıştır,
- Açıklıklara göre risk tanımlaması yapılmıştır,
- Bu risklere göre mevcut durumdaki kontroller tanımlanmıştır,
- Risklerin ortadan kaldırılması yada bertaraf edilmesi için planlanan kontroller tanımlanmıştır,
- Fayda-maliyet analizi yapılmıştır,
- Hedeflenen risk düzeyi tanımlanmıştır,

şeklinde sırayla yürütülecek çalışmalar neticesinde risk analizi süreci tamamlanmış olmaktadır.

2.3. Maliyet-Etkinlik Değerlendirmesi

Yukarıda Çizelge-2'de tariflenmiş olan risk düzeylerine göre kabul edilebilir risk olarak tanımlanan riskler dışında kalan tüm riskler için iyileştirmelerin maliyet-etkinlik değerlendirmesi yapılmıştır. Bu değerlendirme iyileştirmenin maliyeti ile tehdidin gerçekleşmesi durumunda oluşacak kayıp ile kıyaslanarak gerçekleştirilir. Maliyet-etkinlik değerlemesi, aşağıdaki skala baz alınarak gerçekleştirilir.

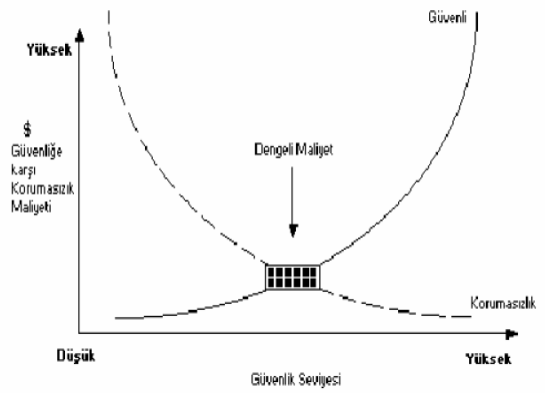
Çizelge 3. Maliyet - Etkinlik düzeyi matrisi

Düzey	Maliyet Durumu
1	İyileştirme maliyetinin, olası zarar düzeyinden çok daha yüksek olduğu durumlarda
2	İyileştirme maliyetinin, olası zarar düzeyinden fazla olduğu durumlarda
3	İyileştirme maliyetinin, olası zarar düzeyine aşağı yukarı denk olduğu durumlarda
4	İyileştirme maliyetinin, olası zarar düzeyinden düşük olduğu durumlarda
5	İyileştirme maliyetinin, olası zarar düzeyinden çok düşük olduğu durumlarda

Çizelge-3'te belirtilen verilere göre önceliklendirme; iyileştirmelerin önceliği sırasıyla maliyet-etkinlik değeri, mevcut risk ve hedeflenen risk düzeyleri değerlerine göre belirlenir.

2.4. Risk değerlendirmesi

e-Devlet Kapısı Projesi bilgi güvenliği yönetimi çalışmaları içerisinde önemli bir yer tutmaktadır. Bu durum özellikle yazılım projesi olarak irdelendiğinde daha da netleşmektedir. Risk değerlendirmesi ile proje başarı performans'ı arasında doğrudan bir bağ bulunmaktadır [5]. Birçok bilimsel çalışma göstermiştir ki; iyi bir risk analizi çalışması; proje varlıklarının tespit edilmesi, risk olasılığı ve projeye olan etkisi, risk önem düzeyi ve fayda-maliyet dengesinin korunması gibi kriterleri kapsamalıdır. Aynı şekilde Şekil-2'de görüleceği üzere yapılan risk analizi neticesinde ortaya çıkan durumun fayda-maliyet dengesi gözetildiğinde güvenliğe karşı korumasızlık maliyeti ile güvenlik seviyesi arasında ters bir orantı görülebilmektedir.



Şekil 2. Güvenlik ve korumasızlık bütçe dengesi [6]

Risk değerlendirme amacıyla kullanılan metot ve modeller, yapılacak değerlendirmenin kapsamına ve risk faktörleri ile ilgili verilerin biçimine göre çeşitlilik gösterir. Risk değerlendirme yöntemleri genel olarak nicel ve nitel yaklaşımlar şeklinde ikiye ayrılır. Nicel yaklaşımda riskin ve riski azaltmak için kullanılacak yöntemlerin finansal maliyeti matematiksel ve istatistiksel yöntemler ile hesaplanır. Bu hesap, olayın gerçekleşme ihtimali, potansiyel kayıpların maliyeti ve alınacak karşı önlemlerin maliyeti kullanılarak yapılır. Eğer elimizde gerçekleşme ihtimali ve maliyetler ile ilgili güvenilir bir bilgi mevcut değilse, riskin düşük, orta ve yüksek gibi daha öznel terimlerle ifade edildiği ve uzmanlık gerektiren nitel yaklaşım kullanılabilir ki; bu çalışma bünyesinde tercih edilen yaklaşım niteldir. Nitel yaklaşımın avantajı riskleri derecelerine göre kolayca sıralayabilmesi ve acil iyileştirme gerektiren alanların tanımlanabilmesidir.

Ancak nitel yaklaşım, sayısal değerler vermediğinden uygulanacak kontrollerin kâr-maliyet analizini yapmak zordur ve uzmanlık gerektiren öznel bir yaklaşım olduğundan farklı zamanlarda farklı sonuçlar verebilir. Bu noktada çalışmada ele alınan proje çıktısı olan risk analizi sonuçları; üst yönetim tarafından onaylanması ile netice alınmıştır. [7]

2.5. Varlık Envanteri ve Sınıflandırması

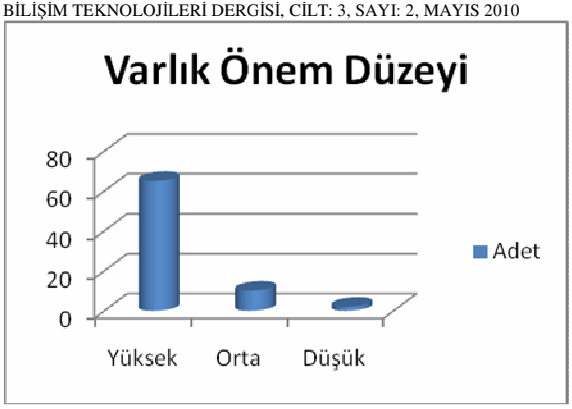
Kuruluş için değeri olan herhangi bir şey'e varlık denilebilmektedir. Varlık envanterine, etkin varlık korumasının gerçekleştiğini temin etmeye yardımcı olması amacıyla; sağlık ve güvenlik, sigorta ve mali (varlık yönetimi) nedenler gibi diğer ticari amaçlar için de gereksinim duyulmaktadır. Varlıkların envanterinin toplanması süreci, risk yönetiminin önemli bir parçasıdır. E-Devlet Kapısı Projesi'nde yapılan risk değerlendirme faaliyetleri içerisinde ilk çıktı olarak "varlık envanteri" karşımıza çıkmaktadır.

Çizelge 4. E-devlet kapısı projesi varlık envanteri örnekleri

No	Varlık Adı	Adedi	Sahibi	Kıymeti	Konumu
1	İnternet Bağlantısı	1	Bilgi İşlem	Yüksek	Gölbaşı
2	Kurum Bağlantıları	Proje bitiminde hedeflenen doğrudan bağlantı sayısı	Ağ ve İletişim	Yüksek	Ulus
3	Kapı Yerel Ağ Altyapısı	8	Ağ ve İletişim	Yüksek	Gölbaşı
4	E-posta Sunucusu	2	Sistem Yönetim	Yüksek	Gölbaşı
5	LDAP Sunucusu	2	Sistem Yönetim	Yüksek	Gölbaşı

Çizelge-4'te görüleceği üzere ülkemize katma değeri oldukça yüksek, ve bilgi toplumuna dönüşüm sürecinde bilgi'yi yönetebilmemizi ve devlet kurumları ile iletişimimizi güçlendirecek olan e-devlet kapısı platform'unun varlık envanterinden alınmış örnek bilgiler bulunmaktadır. Envanterin tamamı incelendiğinde 77 ayrı varlık tespit edilmiş ve proje yapılanması içerisindeki sahibi, proje açısından kıymeti/değeri, konumu gibi bilgileri içeren bir envanter çıkarılmıştır.

E-Devlet kapısı projesi bünyesinde yapılan çalışmada varlık envanterinin tamamı incelendiğinde üç seviye (yüksek, orta, düşük) şeklinde kıymetlendirilmiş, 77 varlıktan 65 tanesi yüksek, 10 tanesi orta ve 2 tanesi de düşük düzeyde kıymete sahip olduğu tespit edilmiştir. %85 'i yüksek düzeyde kıymete sahip olan bu envanter, ülkemizde bilgi toplumuna giden yolda e-devlet kapısı projesinin sadece sonuçlarının topluma yansıması itibarıyla değil aynı zamanda mevcut durumunun da önem katsayısının yüksek olması itibarıyla manidardır. Bu durum Şekil-3'te görülebilecek şekilde özetlenmiştir.



Şekil 3. Adet ve varlık önem düzeyi ilişkisi

Tehdit Tanımlama; spesifik bir zayıflık, sistem adına olumsuz bir kazaya sebep olacak tetikleyici bir davranış, potansiyel bir tehdit kaynağıdır. Burada yapılması gereken en önemli iş; potansiyel tehdit kaynaklarının tespit edilerek bir tehdit listesi oluşturmaktır. Sisteme zarar vermesi muhtemel bu tehditler;

- Doğal (Sel baskınları, Depremler v.s),
- Çevresel (Binaya ait borulardan birinin patlaması ve sistem odasındaki bilgisayarlara zarar vermesi),
- İnsan (Çalışan personel kasıtlı olarak sisteme zarar verebilir, kötü niyetli kişiler sisteme zarar verebilir veya personel istemeden / bilmeden sisteme zarar verebilir)

şeklinde olabilmektedir.

2.6. Zayıflıkların/Zafiyetlerin Tanımlanması

Hedef; sistemde olası zayıflıkların/zafiyetlerin tespit edilmesi ve bunun istismar edilerek potansiyel bir tehdit kaynağı olup olmama durumunun tanımlanması ile ilgili bir liste çıkarmaktır. Çıkarılmış olan bu liste risk analizi sürecinde karşılaşılacak olan etkenlerin tanımlanmasında, fayda maliyet analizinin yapılması aşamalarında oldukça katma değer sağlamıştır.

2.7. Tehdit Olasılıklarının Belirlenmesi

Olasılıklar belirlenirken tehdit kaynaklarının motivasyonlarının ve yeteneklerinin, sistemin doğal zayıflıklarının, mevcut kontrollerin etkinliğinin değerlendirilmesinin düşünülmesi gerekmektedir.

2.8. Mevcut ve Hedeflenen Kontrollerin Tanımlanması

Varlıkların, tehdit, zafiyet gibi nesnel tanımlamaların yapılması sonuç ve olasılık kriterleri neticesinde ortaya çıkan risk düzeyi ile birlikte ana sistemin ayakta kalabilmesi için kurum ya da kuruluşun hali hazırda yaptığı kontrollerin sonuca ne kadar etkisi olduğunu tespit etmek açısından önemlidir. Bu noktada ortaya çıkan etkinin yeterli bulunmaması durumunda mevcut risk'in azaltılması yada ortadan kaldırılması amacıyla yeni kontroller tanımlanması gerekmektedir. Belirlenecek kontrollerin fayda-maliyet dengesinin iyi kurgulanması bu süreçte etkin rol oynamaktadır.

2.9. . Kabul Edilen Riskler

Başka bir ifade ile iyileştirmenin mümkün olmadığı riskler şeklinde tanımlama yapılabilmektedir. Tespit edilmiş olan 434 adet risk içerisinde yönetim, proje ekibi ve bilgi güvenliği lideri'nden oluşan bir komite tarafından karar verilen risklerdir.

2.10. Ele Alınacak Riskler

Ele alınması hedeflenen riskler ve ilgili kontrollere ilişkin hedeflenen iyileştirmeler bu kısımda verilmektedir. Riskler sırası ile hedeflenen risk düzeyi (azalan), kontrol maliyet etkinliği (azalan) ve mevcut risk düzeyi (azalan) sırası ile verilmiştir. Bir sonraki aşamada da bu risklerin giderilmesi için önceliklendirilmiş iyileştirme planları oluşturulmaktadır. Tespit edilen riskler üzerinden hareketle iyileştirme ve risk azaltma planları yapılmış ve Çizelge-5'te aktarılmış olan önceliklendirilmiş riskler ve planlanmış kontrol'ler bulunmaktadır.

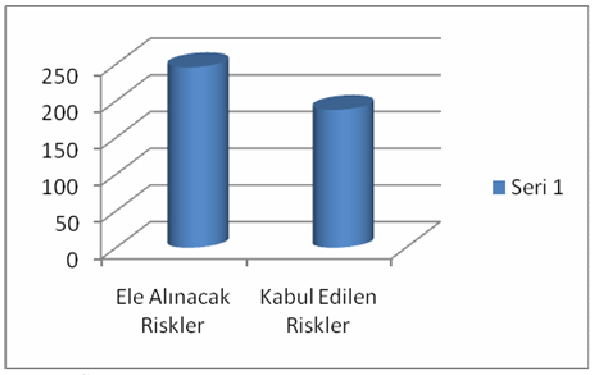
Çizelge 5. Önceliklendirilmiş riskler ve planlanan kontroller

Sıra No	Planlanan Kontrol
1	İşlem kaydı tutulması
2	Merkezi kayıt sunucusu kullanımı
3	Değişiklik kontrol prosedürü
4	Güçlü kimlik doğrulaması
5	Etkin güncelleme yönetimi
6	Bütünlük denetimi yazılımı ile kontrol
7	Periyodik yedekli çalışma testi
8	Zafiyet veritabanlarının düzenli incelenmesi
9	Acil durum müdahale planlaması
10	Kabinet'lerin kilitli tutulması
11	Görev kritik PC'ler ve Laptop'lar için imaj alınması
12	Görev kritik avuç içi sistemler için imaj alınması
13	Bağlantı yedeklemesi
14	Servis sağlayıcının DoS koruması
15	Uç sistem güvenliği ve NAC
16	Disk şifrelemesi
17	Şifrelenmiş yedekleme
18	Sözleşmelerin bilgisayar dosyası olarak saklanması
19	Veri yedeklemesi
20	Disklerin başka kullanıcılar ile paylaşılmaması
21	Temiz masa politikası uygulaması
22	Arşiv sorumlusu atanması ve fiziksel erişim kontrolü

Çizelge 5. Önceliklendirilmiş riskler ve planlanan kontroller (Devamı)

Sıra No	Planlanan Kontrol (Devamı)
23	Yedekleme prosedürü oluşturulması
24	Kablo kanallarının güvenliğinin sağlanması
25	E-posta limitlerinin tanımlanması
26	Tespit edilmiş kritik bilgisayarların yalnızca kurum uzmanları nezaretinde/tarafından kullanılması
27	Yedeklerin FKM'ne gönderilmesi
28	PKI yönetimi için ikili kontrol

Yapılan değerlendirme ve analizler neticesinde e-devlet kapısı projesi bünyesinde tespit edilen 434 adet risk'ten 188 tanesi kabul edilmiş risk'tir. Yani proje yönetim ekibi ile yapılan toplantılarda projenin genelini zor durumda bırakmayacak, projenin devamlılığına engel teşkil etmeyecek ve değerlendirmeye alındığı takdirde sonucun maliyeti'nin, sonucun faydasından büyük olduğu risklerdir. Geriye kalan 246 risk ise ele alınmaya değer, projenin genelini tehlikeye atabilecek düzeyde ve proje yönetimi ekibi ile değerlendirildiğinde sonucun maliyeti, sonucun faydasından büyük olmasına rağmen yapılma zorunluluğu olan risklerdir. Bu durum Şekil-4 'de özetlenmiştir.



Şekil 4. Kabul edilen ve ele alınacak riskler

3. SONUÇ

Bilgi ve iletişim teknolojileri içerisinde sıklıkla yer alan açıklıklardan kaynaklanan tehditlerin bilişim sistemlerine farklı seviyelerde zararı dokunacak ve bunlar değer kaybı olarak karşımıza çıkacaktır. Her bir tehdidin varlığa ne oranda değer kaybettirdiği bilgisi ile tehditlere göre riskler bulunabilir ve değer kayıplarının hesabından riski hesap etmek mümkün hale gelir. Bu çalışmada nitel değerler ile risk hesabı yapan bir model önerilmiş ve gerçek bir proje üzerinden model gerçeklenmiştir.

Bu çalışmada bilgi güvenliği ve risk değerlendirme uygulamalarında çok yaygın bir kullanım alanına sahip olan model, metodoloji ve standartlardan oluşan bir yöntem üzerinden, e-devlet kapısı projesi ele alınmıştır. Teknolojik gelişmeler sonucu, bilgi üretme, üretilmiş bilgiyi saklama ve yönetme artık çağımızın en önemli öğelerindendir. Bu noktada doğal olarak bu evrelerden geçmiş bilginin güvenliği çeşitli risk parametreleri ile karşı karşıyadır. Çalışma neticesinde;

- Proje ile ilgili varlık envanteri çıkarılmıştır.
- Projenin hayata geçirilmesi sürecinde yüzlerce risk tespit edilmiştir.
- Bilgi güvenliği ve risk yönetimi ile ilgili bir süreç tanımlanmış, model ortaya konulmuş ve bu model üzerinden proje hayata geçirilmiştir.
- Tanımlanmış model üzerinde; kabul edilen ve edilmeyen riskler belirlenmiş, fayda-maliyet analizi yapılmıştır.

gibi bulgular sonucunda bilgi ve iletişim teknolojileri alanında ülkemizin en önemli projelerinden birisinde yapılan uygulama projesi paylaşılmıştır. Ayrıca; bilgi güvenliğinin sağlanmasında risk yönetimi sürecinde sistemsel yaklaşım; risklerin tanımlanması, tahmin edilmesi, değerlendirilmesi, bilgi teknolojileri varlıklarının ve bu varlıklara ait açıklıkların ve olası zafiyetlerin ortaya çıkarılması açısından çok önemlidir.[8] Başka bir noktadan konuya bakıldığında risk yönetimi; proje yönetimi ve e-dönüşüm gibi süreçlerin başarıyla sonuca ulaşmasında oldukça fayda sağlamaktadır. Projeyi veya süreci başarıya götürecek alternatif çözümlerin tespit edilmesinde, proje hedeflerine ulaşma olasılığını artırmada, başarı kriterlerini belirlemede, karşılaşılabilecek sürprizleri ortadan kaldırmada, varsayımları tespit etmede, mükerrer iş yaparak maliyetlerin artmasını engellemede oldukça faydalı olduğu kabul görmüştür. [9]

İnternet teknolojileri üzerinden temin edilen raporlama içerikleri, biri diğerinin müşterisini çalmaya çalışan bankalar, VISA raporlarına yansımış kredi kartı işlemleri artan vatandaşlar, uydu yayını ya da kablolu yayın hizmeti veren şirketlerin birbirinin akıllı kart teknolojilerini kopyalamaya çalışması veya hukuki zemini tam olarak oturtulamamış "siber alem"in kontrol altına alınması gibi bilgi ve iletişim teknolojileri ile ister istemez ilgilenmek zorunda olan biz vatandaşları her gün bekleyen ya da karşılaştığımız sorunlardan ötürü bilgi güvenliği önem arz etmektedir[10].

Her geçen gün e-toplum olma yolunda hızla ilerleyen ve e-devletleşme çalışmalarını sürdüren ülkemizde, maalesef bilgi güvenliğinin öneminin kamu veya özel sektör tarafından kavranmadığı veya yüksek seviyede bir farkındalığın oluşmadığı tespit edilen en önemli bulgulardan birisidir.

KAYNAKLAR

[1] İnternet: Bilgi Toplum Stratejisi ve Eki Eylem Planı, http://mevzuat.dpt.gov.tr/ypk/2006/38.htm, Devlet Planlama Teşkilatı, 12.04.2010.

[2] M. Acar, E. Kumaş, "Kamu Hizmetlerinin Sunumunda Dönüm Noktası: e-Devlet, e-Dönüşüm ve Entegrasyon Standartları", 17. İstatistik Araştırmalar Sempozyumu Bildiriler Kitabı, 17(1), 1-18, 2008.

[3] İnternet: Digital Agenda for Europe, http://ec.europa.eu/information_society/digital-agenda/index_en.htm., 12.06.2010.
[4] Türk Standartları Enstitüsü, "Bilgi Teknolojisi-Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri-Gereksinimler TS ISO / IEC 27001:2005", Ankara, 2006.
[5] W. Han, S. Huang, "An Empirical Analysis of Risk Components and Performance on Sofware Projects", The Journal of Systems and Software, 80(1), 42-50, 2006.
[6] E. Kumaş, "e-Devlet Kapısı ve Risk Değerlendirme Metodolojisi", **Türkiye'de İnternet Konferansı – İnet-tr**, Ankara, 203-308, 2007.
[7] H. Takçı, T. Akyüz, A. Uğur, R. Karabağ, I. Soğukpınar, "Bilgi Güvenliği Yönetiminde Varlıkların Risk Değerlendirme İçin Bir Model", **Ağ ve Bilgi Güvenliği Ulusal Sempozyumu**, Ankara, 6-10, 2010.
[8] M. Gerber, R. Von Solms, "Management of Risk in the Information Age", Computer & Security, 24(1), 16-30, 2005.
[9] P. L. Bannerman, "Risk And Risk Management in Software Projects: A Reassessment", The journal of systems and software, 81(1), 2118-2133, 2008.
[10] R. J. Anderson, "Security Engineering: A Guide to Building Dependable Distributed Systems", John Wiley&Sons, Cambridge, U.S.A., 2001.