Bilgi Güvenliği Yönetim Sistemi için Süreç Tabanlı Risk Analizi

Bilge Karabacak[1] Dr. Sevgi Özkan[2]

[1]Enformatik Enstitüsü, Orta Doğu Teknik Üniversitesi, Ankara
[2]Enformatik Enstitüsü, Orta Doğu Teknik Üniversitesi, Ankara

[1]e-posta: bilge@uekae.tubitak.gov.tr [2] e-posta: sozkan@ii.metu.edu.tr

Özetçe

Günümüzde, birçok kuruluş Bilgi Güvenliği Yönetim Sistemi (BGYS) kurmak ve bu yönetim sistemini TS ISO/IEC 27001 sertifikası ile belgelendirmek istemektedir. BGYS'nin hedeflediği kapsam tüm kurum ve iş süreçleri olsa da bu isteklerin genellikle kurumların bilgi işlem birim temsilcilerinden veya bilgi işlem biriminin bağlı olduğu üst yöneticilerinden geldiği görülmektedir. TS ISO/IEC 27001 standardı, belirli bir kapsam dâhilinde iş süreçlerini dikkate alan bir risk analizinin gerçekleştirilmesini zorunlu kılmaktadır. İstekler bilgi işlem birimlerinden geldiği için birçok BGYS kurulum çalışmasında kapsam bilgi işlem süreçleri olarak belirlenmektedir. Diğer taraftan bilgi işlem kapsamında gerçekleştirilmesi planlanan risk analizi sürecinde genellikle sadece donanımlara ve yazılımlara odaklanılmaktadır. Bu durumda ise, yönetimsel birçok risk göz ardı edilebilmektedir. Bu çalışmada, bir BGYS kurulum çalışmasında süreçlerin, süreçte yer alan varlıkların, varlıklardaki açıklık ve tehditlerin nasıl ifade edilebileceğine yer verilmiş ve süreç modeli kullanılarak nasıl risk analizi yapılabileceği konusunda bir öneri getirilmiştir. Önerilen metodun, özellikle bilgi işlem süreçlerinin kapsam dâhilinde olduğu Bilgi Güvenliği Yönetim Sistemi kurulumu çalışmalarında etkin bir şekilde kullanılabileceği değerlendirilmektedir.

1. Giriş

Son yıllarda, ülkemizdeki kamu kurumları ve özel şirketler TS ISO/IEC 27001 standardına daha çok ilgi göstermeye başlamışlardır [1]. TS ISO/IEC 27001 standardının sertifikasyonunun olması bu ilgiyi artırmaktadır. TS ISO/IEC 27001 sertifikasyonunun yakın bir gelecekte tüm dünyada büyük oranda yaygınlaşacağı öngörülmektedir [2]. Günümüzde, birçok kuruluş TS ISO/IEC 27001 sertifikası alma niyetinden bahsetmektedir. Bunun yanı sıra bazı kuruluşlar belgelendirme için gerekli işlemlere devam etmekte ve bazıları da hâlihazırda almış bulunmaktadır.

TS ISO/IEC 27001, etkili bir Bilgi Güvenliği Yönetim Sistemi (BGYS) kurulması ve yönetilmesi için gerekli adımlara yer vermektedir. TS ISO/IEC 27001, kuruluşun ticari riskleri bağlamında belgelendirilmiş bir BGYS'nin kurulması, uygulamaya konulması, işletilmesi, takip edilmesi, incelenmesi, bakımı ve geliştirilmesi için gereklilikleri tanımlar. Söz konusu gereklilikleri yerine getirmek için atılması gereken en önemli adım, riskleri belirlemek için bir risk analizi yapmaktır. TS ISO/IEC 27001, belirli bir risk analiz yöntemini önermemektedir, bunun yerine bu sürecin zorunlu olduğunu ve "risk değerlendirmesine yönelik sistematik bir yaklaşım" tanımlanmasını gerektiğini belirtmektedir [1].

Standardın 4.2.3-d maddesinde "iş hedefleri ve iş süreçlerindeki değişikliklere göre risk değerlendirmesinin gözden geçirilmesi"nin gerekliliği vurgulanmıştır. Ayrıca standartta, bir kuruluşun BGYS'sini kurmak, gerçekleştirmek, işletmek, izlemek, sürdürmek ve iyileştirmek için süreç yaklaşımının benimsendiği ifade edilmektedir. TS ISO/IEC 27001, bütün uygulama boyunca iş süreçlerini dikkate almayı zorunlu kılar. Kaynakları kullanan ve girdileri çıktılara dönüştüren her türlü etkinlik süreç olarak düşünülebilir. Bir kuruluştaki BGYS'nin tasarımı ve uygulamaya konulması, söz konusu kuruluşun süreçlerinden etkilenir [1]. TS ISO/IEC 27001'i uygularken süreç yaklaşımı takip edilmeli bu kapsamda süreçlerin tanımlanması, işleyişlerinin yazılı hale getirilmesi, modellenmesi ve süreçlerin karşılıklı etkileşimlerinin ortaya konması işlemleri başarılı bir şekilde gerçekleştirilmelidir. Risk analizi BGYS'yi kurmanın hayati öneme sahip bir parçasıdır, bundan dolayı süreç yaklaşımı, risk analiz yöntemine de uygulanmalıdır. Süreç yaklaşımı bulunmayan bir risk analizi yönteminin, BGYS'ye uyumda ciddi zorluklar çekeceği söylenebilir.

Bu çalışmada, TS ISO/IEC 27001'in gereklilikleri dikkate alınarak, süreç modellemesi tabanlı bir risk analizi yöntemi önerilmiştir. Önerilmiş olan risk analizi yöntemi, özellikle ülkemizdeki kamu kurumlarının da talep ettikleri, bilgi işlem süreçlerini kapsamı içine alan Bilgi Güvenliği Yönetim Sistemleri kurulumları için tasarlanmıştır.

2. Bilgi Güvenliği için Risk Analizi Yöntemleri

Risk önceden bilinen somut bir değer değil, bir olasılık değeridir. Bu nedenle risk analizi bir olasılık hesabıdır ve karmaşık bir süreç olabilmektedir. Bilgi teknolojileri söz konusu olduğunda, risk analizi sürecinin karmaşıklığı daha da artmaktadır. Bilgi teknolojileri açısından risk, basit bir olasılık değeri değildir. Risk, bir varlıktaki bir açıklığın bir tehdit tarafından kullanılma olasılığıdır. Böylece risk; varlık, açıklık ve tehdit olmak üzere üç adet girdiye bağımlıdır.

$$\text{Risk} = f(\text{Varlık, Açıklık, Tehdit}) \quad (1)$$

Formüldeki f fonksiyonu, risk modelini ifade etmektedir. Bu modelin üç adet temel girdisi vardır ve bu fonksiyonun (modelin) çıktısı da risk değeridir.

Yapılan literatür taramasında, bilgi güvenliği risk analizi konusunda bayes ağları, bulanık mantık, simülasyon, hata ağaçları gibi matematiksel yöntemlerin önerildiği görülmüştür [3, 4, 5]. Bu tip matematiksel modeller, yer aldıkları yayınlarda da belirtildiği

gibi özelleşmiş bir problemin çözümünde etkin olabilir. Bu yöntemlerin BGYS kurulumu kapsamındaki risk analizi çalışmasında kullanılması durumunda sürecin karmaşıklığı yönetilemez boyuta gelebilecektir. Diğer taraftan unutulmamalıdır ki, bilgi güvenliğinin az bir bölümü teknik ve teknolojik daha kapsamlı bölümü ise süreçler ve sosyal ilişkiler ile ilgilidir [6, 7]. BGYS kurulumu çalışmalarında bulunmuş olan kişiler bu gerçeği doğrulayacaklardır. Güvenlik duvarına anlık mesajlaşmayı engelleyen bir kural koymak çok kolay iken, bunu bir kurum politikası olarak uygulamak oldukça zordur. Bu işlemin kolay olan kısmı bilgi güvenliğinin teknik boyutunu, zor olan kısmı ise sosyal boyutunu temsil etmektedir. Risk analizi gibi BGYS'nin önemli bir kısmını oluşturan önemli bir sürecin de bu gerçek ile uyumlu olması başarı için gerekli bir şarttır.

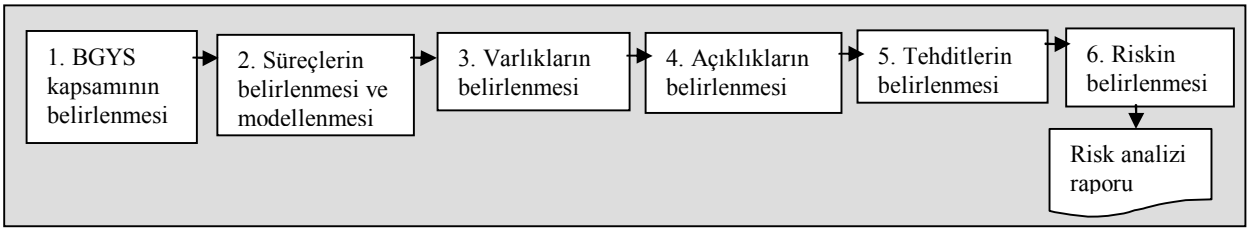
Bilgi güvenliği risk analizi sürecinde kullanılan ve bu süreçteki birçok aktiviteyi otomatikleştiren çok sayıda yazılım mevcuttur. Bu yazılım araçlarının en tanınmışları, nicel risk modellerine dayalı olan CRAMM [8] ve RiskWatch [9] yazılımlarıdır. Bu yazılımlar, BGYS kapsamındaki risk analizlerinde de kullanılabilmektedir. Risk analizi sürecinde yazılım kullanılmasının bazı dezavantajları olabilmektedir. Öncelikle, böyle bir yöntemin maliyeti genellikle yüksek olmaktadır. Maliyet kalemi içerisinde sadece yazılımın tedarik maliyetinin olmadığı, destek, güncelleme ve eğitim faaliyetlerinin de olduğu unutulmamalıdır. İkinci dezavantaj, risk analiz sürecinin ana çerçevesinin yazılım tarafından belirlenmesidir. Böylece, risk analizi sürecinde kuruma özel yapılması gereken bazı değişiklikler yapılamayabilmektedir [10].

Devlet Planlama Teşkilatı Müsteşarlığı Bilgi Toplumu Dairesi tarafından hazırlanmış olan Bilgi Toplumu Stratejisi Eylem Planı'nda yer alan 88 numaralı madde Ulusal Bilgi Sistemleri Güvenlik Programı'nı tanımlamaktadır [11]. Söz konusu programın sorumlu kuruluşu olarak TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, dört adet kamu kurumuna Bilgi Güvenliği Yönetim Sistemi kurulumu danışmanlığı vermiştir. Bu çalışmalarda, kurulması planlanan bilgi güvenliği yönetim sistemlerinin kapsamı temel olarak bilgi işlem süreçleri olarak belirlenmiş ve bilgi işlem birimlerinin temsilcileri ile çalışılmıştır. Bu çalışmalar esnasında BGYS kapsamının belirlenmesinin ardından öncelikle risk analizi süreci için temel bir girdi olan varlık envanteri oluşturulmuştur. Bu aşamada, bilgi işlem personelinin varlık envanterini bir ayniyat veritabanı olarak algıladığı ve sonuç olarak bu envantere sadece bilgi işlemin sahip olduğu donanım/yazılımları yazdığı ve bilgi varlıklarını listelemekte zorlandıkları görülmüştür [12]. Risk analizi sürecinde, varlıklardaki açıklıklar ve bu açıklıkları kullanan tehditler ortaya konulduğu için, varlık envanterinde sadece bilgi işlemin işlettiği teknolojik varlıkların yer alması risk analizinin eksik sonuçlar vermesine yol açacaktır. Bu tip eksik risk analizleri, bilgi güvenliğinin daha çok teknik boyutlarına yoğunlaşacak ama sosyal ve süreçler ile ilgili boyutlarını ihmal edecektir.

Ülkemizde özellikle kamu kurumlarının bilgi işlem birimleri, BGYS konusuna ilgi göstermekte ve bu yönetim sistemini kurmak istemektedirler. Gerçekte, BGYS bilginin işlendiği her yere uygulanabilecek olan bir sistemdir, sadece bir bilgi işlem aktivitesi değildir [12]. Ancak, ülkemizde bilgi güvenliği yönetişimi ile ilgili yasal altyapı olmadığı için bir kamu kurumunun tüm birimlerini içine alan bir BGYS kurmak oldukça güçtür ve henüz böyle bir örnek bulunmamaktadır. Öte taraftan, bu sisteme ilgi gösteren bilgi işlem birimlerinin de BGYS'nin teknik bir altyapı olmadığını bilmeleri gereklidir. Bu makalede önerilen süreç tabanlı risk analizi metodunun, BGYS'ye ilgi gösteren bilgi işlem birimlerinin konuya sadece teknik açıdan yaklaşmalarını engelleyeceği ve süreçleri de dikkate alarak çalışma yapmalarına imkan vereceği düşünülmektedir. Önerilen metot önümüzdeki senelerde yasal altyapının da oluşturulması ile beraber hem birçok kuruma hem de kurumlardaki bilgi işlem birimleri dışındaki diğer birimlere yaygınlaşması öngörülen BGYS çalışmalarına hazırlıklı olmalarına katkı yapacaktır.

3. Süreç Tabanlı Risk Analizi Yöntemi

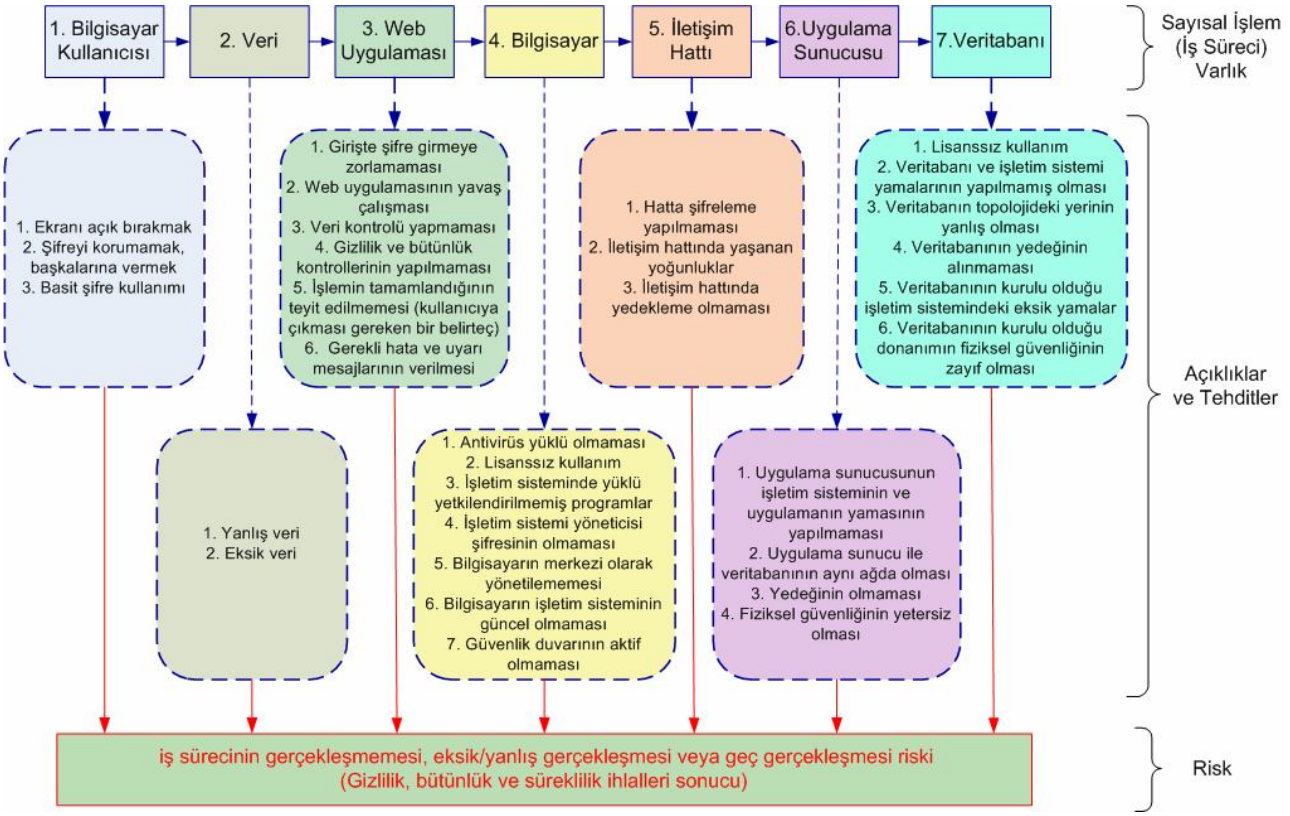
Risk analizi çalışmaları belirlenmiş olan BGYS kapsamı dâhilinde gerçekleştirilir. BGYS'nin kapsamı aynı zamanda risk analizinin de kapsamıdır. Aynı kapsamın, varlık envanterinin oluşturulması esnasında da dikkate alınması gerekir. Birçok BGYS çalışmasında kapsamın belirlenmesinin ardından, varlık envanteri oluşturulmasına geçilmektedir. Önerilen metotta, BGYS kapsamının belirlenmesinin ardından, varlık envanterine geçilmeden önce bu kapsam içerisinde yer alan süreçlerin ortaya konulması ve modellenmesi önerilmektedir. Süreçleri oluşturan yapıtaşları varlıklardır. Bu nedenle, süreçlerin belirlenmesi ve yazılı hale getirilmesi varlıkların daha sağlıklı ve eksiksiz bir şekilde belirlenmesini de sağlayacaktır. BGYS kapsamının belirlenmesinin ardından doğrudan varlık envanterinin oluşturulması aşamasına geçilmesi, bilgi işlem personelinin sadece donanım ve yazılımlara odaklanmasına yol açmaktadır. Önerilen metotta ise, modellenmiş süreçlerden yola çıkılarak belirlenmiş olan varlıklardaki açıklıklar ve bu açıklıklar kullanan tehditler ortaya konmaktadır. Risk analizinin son adımında ise, belirlenmiş olan varlık, açıklık ve tehditlere değerler verilerek risk hesaplanmakta ve risk analizi süreci tamamlanmaktadır. Önerilen risk analizi metodunun genel akış diyagramı Şekil-1'de verilmiştir.



Şekil 1: Öngörülen yöntemin genel yapısı

Süreçler, girdileri çıktılara dönüştüren organize faaliyetler bütünüdür. Bir süreç, bir ürünün ya da bir hizmetin üretilmesine ya da

teslimatına katkıda bulunan değerler zinciri olarak görülebilir. BGYS kapsamındaki bilgi işlem süreçleri genellikle kolay bir şekilde modellenebilen ve yazılı hale getirilebilen süreçlerdir. Ayrıca, önerdiğimiz risk analizi metodunda, süreç modellemesi için karmaşık bir yöntem önerilmemiştir. ISO 9001 gibi bir yönetim sisteminin olmadığı kurumlar genellikle fiilen gerçeklemiş oldukları iş süreçlerini yazılı hale getirmemişlerdir. Bu nedenle, karmaşık süreç modelleme teknikleri BGYS çalışmalarını zorlaştırabilecektir. Bir bilgi işlem aktivitesini veya bilgi işlem altyapısını kullanan bir bilgisayar kullanıcısının yaptığı işlemi modellemek akış diyagramları ile oldukça kolay olmaktadır. Akış diyagramları en çok bilinen ve uygulama kolaylığı olan süreç modelleme yöntemidir. Sistemin bütüncül yapısını göstermede ve bu yapı içerisinde işlerin ve bilginin akışını izlemede faydalıdır [13]. Şekil-2'de bir bilgisayar kullanıcısının veri girişi modellenmiştir. Birçok kurumda, kurumun kritik bilgisini içerdiğinden dolayı veritabanları en kritik varlıklardır. Veritabanlarına veri girişi genellikle kurum personeli tarafından yapılan günlük bir iş sürecidir. Şekil-2'de bu kritik işlem yedi adet süreç kutusu kullanılarak akış diyagramı metodu ile basit bir şekilde modellenmiştir. Bu basit modelleme, veri giriş sürecinde hangi bilgi işlem elemanlarının kullanıldığını ortaya koymuştur.



Şekil 2: Örnek bir süreç modeli ve modelin kullanılarak risk analizi yapılması

Akış diyagramındaki her bir süreç kutusu aslında bir varlığa işaret etmektedir. Böylece akış diyagramı kullanarak hem varlıklar listelenmiş hem de bu varlıkların birbirleri ile olan ilişkileri ortaya konulmuştur. Özetlemek gerekirse, bilgisayar kullanıcısı, evraktaki veriyi bilgisayarındaki web uygulamasını kullanarak sayısallaştırır, bu aşamada, veri iletişim hattından geçerek uygulama sunucusuna gelir, uygulama sunucusu da yine iletişim hattını kullanarak veritabanına verinin yazılmasını sağlar. Bu işlemde bilgisayar kullanıcısı da dahil olmak üzere adı geçen her şey birer varlıktır. Varlıkların süreç içerisinde gösterilmesi ve listelenmesinin ardından ikinci aşama olarak bu varlıklardaki açıklıklar ve bu açıklıkları kullanabilecek tehditler ortaya konur. Bu da yine akış diyagramı kullanılarak yapılır. Makalenin başında bahsedildiği gibi klasik varlık envanteri oluşturulurken yapılan önemli hatalardan birisi olan, varlık envanterinde sadece teknik bileşenlerin geçmesi hatası tekrarlanmadığı için bilgisayar kullanıcısından, girilen verinin doğruluğuna ve kullanıcının bilgisayarına kadar birçok alanda açıklık ve tehditler saptanmış olur. Belirlenmiş olan her bir açıklık ve tehdit Şekil 2'de de gösterildiği gibi akış diyagramı kullanılarak modellenmiş olan sürecin gerçekleşmemesi, eksik/yanlış gerçekleşmesi veya geç gerçekleşmesi gibi birer sebep olacaktır. O halde, iş sürecinin her aşamasında varlıkları etkileyen tehditleri ve bu varlıklardaki açıklıkları engellemek gereklidir.

Şekil 2'de gösterilen adımların kapsam dahilindeki tüm süreçler için tamamlanması ile beraber, Şekil 1'deki genel akış diyagramındaki 2, 3, 4 ve 5 numaralı adımlar da gerçekleştirilmiş olacaktır.

Bu aşamadan sonra, birçok kaynakta önerilen ve standart olarak kullanılan (2) numaralı formül ile risk değeri hesaplanır ve risk analizi tamamlanır [14, 15, 16].

$$\text{Risk} = \text{Tehdidin etki derecesi} \times \text{tehdidin gerçekleşme ihtimali} \qquad (2)$$

Risk analizi sürecinin bu son aşamasının da tamamlanması ile birlikte Şekil 1'deki 6 ve 7 numaralı adımlar tamamlanmış olacaktır. Yer darlığından ve makalenin asıl konusu olmadığından dolayı bu aşama ile ilgili ayrıntılara makalede yer verilmemiştir.

Bu aşama ile ilgili olarak Bilgi Güvenliği Kapısı'daki BGYS kılavuzlarına başvurulabilir [17].

4. Tartışma

Bilgi güvenliği risk analizi konusunda akademik yayınlarda birçok metot önerilmektedir. Akademik yayınlar genellikle dar problem alanlarına yönelmekte ve belli bir durum için daha etkin çözüm önerileri getirmeye çalışmaktadır. Bu nedenle akademik yayınlardaki öneriler kurumsal beklentileri karşılayacak düzeyde olmamaktadır [18]. Bilgi güvenliği risk analizi sürecini otomatikleştirmeye ve kolaylaştırmaya yönelik birçok ticari yazılım mevcuttur. Ticari yazılımlar ise her kurum tarafından tercih edilmemektedir. Bunun nedenleri, yazılımın pahalı olması, tam olarak kurumun ihtiyaçlarına yönelememesi, yazılımın karmaşık olması ve kurumun yazılım çerçevesinde kalmak istememesi olabilmektedir [19].

Akademik yayınlar ve ticari yazılımlar risk analizi sürecinin belli başlı zorluklarına değinirler, bu zorlukların nasıl aşılabileceği, risk analizi sürecinin nasıl etkin ve kolay yürütülebileceği konusunda öneriler getirirler [20].

Bilgi güvenliği risk analizi sürecinin başlıca zorlukları arasında:

1. Bilgi güvenliği riskinin, varlık, açıklık ve tehdit değerlerini girdi olarak alan karmaşık bir olasılık fonksiyonunun sonucu olması,
2. Bilgi güvenliği risk analizi kapsamındaki en temel ve önemli varlık olan bilginin soyut olması ve bilginin birçok değişik formda bulunması,
3. Bilgi sistemlerinin karmaşık ve yaygın bir yapıda olması, varlık, açıklık, tehdit ve karşı önlemler arasındaki birçok çapraz ilişkinin olması sayılabilir.

İdeal bir bilgi güvenliği risk analizi sürecinin özellikleri:

1. Karmaşık olmaması,
2. Maliyet etkin olması,
3. Hızlı sonuçlar vermesi,
4. Objektif sonuçlar vermesi,
5. İş süreçleri odaklı olması,
6. Bilgi odaklı olması,
7. Kurum personelinin katılımına imkân vermesi şeklinde sıralanabilir.

Bu makalede, bilgi güvenliği risk analizinin zorluklarını göz önüne alan ve risk analizi sürecinden beklenen özellikleri yerine getirebilecek süreç tabanlı bir risk analizi metodu önerilmiştir.

BGYS kapsamı dâhilindeki süreçlerin akış diyagramları ile modellenmesi sonucunda bilginin akışı ve değişik formlara girişi kolaylıkla görülebilecektir. Aynı diyagram içerisinde varlıkların belirlenmiş olması ve bu varlıkların sahip oldukları açıklıkların ve bu açıklıkları etkileyen tehditlerin de belirlenmesi risk analizi ile ilgili zorlukları hafifleten etkenledir.

Önerilen süreç tabanlı risk analizi metodu, karmaşık bir yapıda değildir. Hâlihazırda kullanılan yöntemlere daha da açıklık getiren bir yapıda tasarlanmış bir yöntem olup maliyet etkin ve hızlı sonuçlar veren bir yöntemdir. Yöntem iş süreçlerine ve bilgiye dikkat çekmekte ve kurum personelinin sürece kolaylıkla katılmasına imkân vermektedir.

Yöntem, kapsamın bilgi işlem süreçleri olarak belirlendiği BGYS çalışmalarında etkin bir rol oynayabilir. Öte taraftan, birçok karmaşık ve büyük iş sürecinin kapsam dâhilinde olduğu BGYS çalışmalarında etkin bir yöntem olarak kullanılamayabilir.

5. Sonuç

Risk analizi, riski tahmin etmek amacıyla yapılan sistematik çalışmalardır. Yapılan risk tahminleri karşı önlemlere karar verilmesi aşamasında önemli bir parametre olarak kullanılırlar. Risk analizi yapılmadan veya eksik yapılarak tesis edilen karşı önlemlerin ihtiyacı karşılayamaması veya gereğinden fazla karşılaması ihtimali büyüktür. Bu nedenle, risk analizi çalışmasının sağlıklı ve etkin bir şekilde yapılması gerekir. Sağlıklı ve etkin bir risk analizi süreci için en önemli şartlardan birisi, risk analizini bizzat kurum çalışanları ile birlikte yapılmasıdır. Bu durum ise, risk analizi sürecinin değişik disiplinlerdeki kişilerin de katılımına imkân sağlayacak şekilde olması gerekliliğini ortaya koymaktadır. Kapsam dâhilindeki kurum personelinin de risk analizi sürecine katılması için en önemli şartlardan birisi de sürecin karmaşık bir şekilde tasarlanmamış olması gerektiğidir. Kapsam dâhilindeki süreçleri modelleyebilen bir risk analizi süreci kurum çalışanlarının beyin fırtınası yapması için uygun bir ortam sağlayacaktır.

Günümüzde, BGYS kurulum istekleri bilinçlenmeden dolayı genellikle kurumların bilgi işlem birimlerinden gelmektedir. Bu da, bilgi işlem süreçlerinin kapsam dâhilinde olduğu BGYS çalışmalarının önünü açmaktadır. Kapsam dâhilindeki süreçleri modelleyebilen bir risk analizi süreci, BGYS'ye sadece teknik çerçeveden bakılmasının da önüne geçecek önemli bir araç olacaktır.

Önerilmiş olan yöntemin TS ISO/IEC 27001 standardındaki gereklilikleri karşılamaktadır. Standart çerçevesinde önerilen metodun kullanılmasıyla oluşturulmuş olan bir BGYS'nin kolaylıkla sertifika alabileceği değerlendirilmektedir.

Akademik kaynaklarda BGYS sertifikalandırma sürecinin son derece zor olabildiği söylenmektedir [19]. Bunun nedeni olarak standardın birçok unsuru aynı anda içermesi ve sertifikasyon için tüm unsurların bulunması gerekliliği gösterilmektedir. Önerilen yöntem, BGYS kurulumu kapsamındaki birçok temel unsuru kapsamaktadır. Bütün bu unsurları, kurum çalışanlarının da katılımı ile maliyet etkin ve hızlı bir şekilde tamamlamak mümkündür.

Önerilmiş olan süreç tabanlı risk analizi yöntemi ile sadece teknik riskler değil, kurumsal, fiziksel, süreçsel ve personel ile ilgili riskler de dikkate alınmaktadır. Standart ve akademik kaynaklar, BGYS'nin kuruluşun ticari riskleri bağlamında kurulması gerektiğini ifade etmektedir [21]. Bu nedenle sadece bilgi işlemin sorumluluğunda olduğu teknik riskler göz önüne alınarak BGYS kurulması beklenen etkiyi göstermeyecektir. Önerilmiş olan yöntem sadece sunucular ve yazılımlar gibi teknik kalemleri ön

plana çıkartmamaktadır, bunun yerine süreçleri vurgulamaktadır. Böylece, söz konusu yöntem kurumsal bakış açısı ile uyum sağlamaktadır.
Son söz olarak önerilmiş olan özelleşmiş bir yazılımın kullanılmadığı, süreç modellemesini içeren ve nitel risk analizi yöntemi kamu kurumları bilgi işlem birimlerinin ihtiyaçlarını karşılayacak şekilde tasarlanmıştır [10].

6. Kaynakça

[1] TS ISO/IEC 27001:2006, Bilgi teknolojisi – Güvenlik teknikleri - Bilgi güvenliği yönetim sistemleri – Gereksinimler
[2] "BS7799 – Slow Uptake by Companies", Computer Fraud & Security, doi:10.1016/S1361-3723(03)03005-7, 2003 (3): 3, 2003
[3] Bilbao A., "TUAR. A Model of Risk Analysis in The Security Field", CH3119-5/92. IEEE, 1992.
[4] Spinellis D., Kokolakis S., Gritzalis S., "Security Requirements, Risks and Recommendations for Small Enterprise and Homeeoffice Environments", Information Management & Computer Security, 7(3): 121-128, 1999
[5] Ru W. G., Eloff J. H. P., "Risk Analysis Modelling with the Use of Fuzzy Logic" Computers & Security, 15 (3): 239-248, 1996
[6] Broderick J. S., "ISMS, Security Standards and Security Regulations", Information Security Technical Report, Sayı II: 26-31, 2006
[7] Booth, M. E., Philip G., "Information Systems Management in Practice: An Empirical Study of UK Companies", International Journal of Information Management, Sayı 25: 287-302, 2005
[8] United Kingdom Central Computer and Telecommunication Agency (CCTA), "Risk Analysis and Management Method, CRAMM User Guide, Baskı 2.0", 2001
[9] RiskWatch, http://www.riskwatch.com, 2005
[10] Karabacak, B., Soğukpınar, I., "ISRAM: Information Security Risk Analysis Method", Computers & Security, Sayı 24: 147-159, 2005
[11] Bilgi Toplumu Stratejisi Eylem Planı (2006-2010), http://www.bilgitoplumu.gov.tr/btstrateji/Eylem_Plani.pdf
[12] Karabacak B., "ISO/IEC 27001:2005 ve Bilgi Güvenliği Yönetişimi - Türkiye Analizi", Bilgi Güvenliği Kapısı, http://www.bilgiguvenligi.gov.tr, 2008
[13] Giaglis M. G., "A Taxonomy of Business Process Modeling and Information Systems Modeling Techniques", The International Journal of Flexible Manufacturing Systems, Sayı 13: 209-228, 2001
[14] National Institute of Standards and Technology (NIST), "Special Publication 800-30: Risk Management Guide for Information Technology Systems", 2001
[15] McEvoy, N., Whitcombe, A., "Structured Risk Analysis", InfraSec 2002, LNCS 2437: 88-103, 2002
[16] United States General Accounting Office (USGAO), "Information Security Risk Assessment", http://www.gao.gov/cgi-bin/getrpt?GAO/AIMD-00-33, 1999
[17] Bilgi Güvenliği Yönetimi Kılavuzları, http://www.bilgiguvenligi.gov.tr/bilgi-guvenligi-yonetimi-dokumanlari/index.php
[18] Tong C.K.S., Fung, K.H., Huang H.Y.H, Chan K.K., "Implementation of ISO17799 and BS7799 in Picture Archiving and Communication System: Local Experience in Implementation of BS7799 Standard", Computer Assisted Radiology and Surgery, Proceedings of the 17th International Congress and Exhibition, Sayı 1256: 311-318, 2003
[19] Solms, B., Solms, R., "Incremental Information Security Certification", Computers & Security, 20(4): 308-310, 2001
[20] Karabacak B., "Kurumsal Bilgi Güvenliğinde Etkin Risk Analizi", Bilgi Güvenliği Kapısı, http://www.bilgiguvenligi.gov.tr, 2009
[21] Posthumus, S., Solms, R., "A Framework for the Governance of Information Security", Computers & Security, Sayı 23:638-646, 2004