Bilgi Güvenliğinde Uygun Risk Analizi ve Yönetimi Yönteminin Seçimi İçin Bir Yaklaşım

A New Approach for Choosing Proper Risk Analysis and Management Method in Information Security

F. Özden Aktaş, İbrahim Soğukpınar

Bilgisayar Mühendisliği Bölümü
Gebze Yüksek Teknoloji Enstitüsü
oaktas@gyte.edu.tr, ispinar@bilmuh.gyte.edu.tr

Özet

Son yıllarda bilgi sistemleri ve ağ teknolojilerinin kullanım alanlarının yaygınlaşmasıyla beraber, bilgi güvenliğinin de önemi artmıştır. Bilgi güvenliği aktivitelerinde anahtar kavram risk analizidir. Sistemlerdeki güvenlik seviyesini tespit etmek ve daha iyi hale getirebilmek için, mevcut riskleri belirleyebilmek, bunları analiz etmek, karşı tedbirler geliştirebilmek, kısacası yönetmek gerekmektedir. Risk yönetiminde uzmanlaşmış yöntemler kullanmak, organizasyonlar için ilerideki çalışmalarına daha planlı bir anlayış getireceğinden faydalı olacaktır. Bugüne kadar geliştirilmiş, karakteristikleri ve uygulanışları farklı pek çok yöntem bulunmaktadır. Bu yöntemlerin salt olarak birbirlerinden üstünlüklerinden bahsedebilmek mümkün değildir. Bir yöntem uygulandığı organizasyona bağlı olarak diğerlerine göre daha avantajlı hale gelebilir. Bu amaçla, organizasyonların kendi ihtiyaçlarına en uygun şekilde cevap verebilecek olan yöntemi seçebilmelerine yol gösterecek araçlara ihtiyaç duyulmaktadır. Bu çalışmada uygun yöntem seçimi için bir yaklaşım önerilmektedir. Önerilen yaklaşım dört adet risk analizi yöntemi üzerinde test edilerek sonuçları verilmiştir.

Abstract

Due to spread in usage of information systems and network technologies, the importance of information security has also increased in recent years. The key concept in information security activities is risk. To determine and improve the security level in the systems, one has to determine the current risks, to analyze them, to generate solution; that is to manage them. Using specialized methods for managing risk would be useful for organizations since it will bring a more planned perspective to their future work. There are several methods developed till now, varying in their characteristics and their applications. It is not possible just to mention the superiority of one over another. A method may be more advantageous than others depending on the organization in which it is applied. For this purpose, there is need to find guiding tools for choosing a method that can satisfy organizations' needs in the most useful way. This article recommends the approach for selecting the proper method. Test results of application are giver in this article for the proposed approach.

1. Giriş

Bilgi; yazılı, elektronik olarak saklı, iletilen veya görüntülü ya da sözlü çeşitli formlarda olabilen ve uygun bir şekilde korunması gereken varlıktır. Diğer önemli iş değerleri gibi, organizasyonlar için bir öneme sahiptir ve bu nedenle de gerektiği şekilde korunmaya ihtiyaç duyar. Bilgi güvenliği, işin devamlılığını, iş kaybını mimimuma indirmeyi, gelirdeki ve iş fırsatlarındaki kârı maksimize etmeyi garantilemek için geniş anlamdaki tehditlerden bilgiyi; genel güvenlik şartları olan gizliliğini, bütünlüğünü, hazır bulunuşluğunu sağlayarak korumaya çalışır [1].

Organizasyonlar, bilgi güvenliğini gerçekleştirmek için olası zayıflıklardan kaçınmaya çalışsalar da, tüm bilgilerini her zaman yüzde yüz güvenli hale getiremezler. Bu yüzden, varlıklar üzerindeki potansiyel zayıflıklara bağlı olarak, sistemler üzerindeki riski yönetmek, bilgi güvenliği aktivitelerinin temel parçasıdır.

Risk yönetimi yaparken, sistemi olumsuz yönden etkileyebilecek şüpheli olaylar tanımlanır, maliyet-fayda dengesi sağlanacak şekilde çeşitli koruyucu önlemler belirlenerek riski ortadan kaldıracak veya azaltacak şekilde uygulanır.

Bilgi güvenliğinin uygulama alanı, günümüzde birçok standartlar, sertifikalar ve risk analiz yöntemleri tasarlanarak genişletilmiştir ve halen de genişletilmeye devam edilmektedir [2]. Vorster ve Labuschagne, mevcut risk analizi yöntemlerini karşılaştıran bir çalışma yapmışlardır [9]. Bu yöntemlerin hepsinin genel hedefi, bilginin güvenlik şartları sağlanarak korunması olmasına karşın, uygulamada izledikleri yol ve kullandıkları metrikler farklılık gösterir. Sözgelimi, bazı risk analizi yöntemlerinde risk elemanının ölçümünde metrik olarak nitel yapılar kullanılırken, bazılarında nicel yapılar kullanılmakta, diğerlerinde ise nitel ve nicel özelliklerin beraberce kullanıldığı karma bir yapı gözlemlenmektedir. Başka bir açıdan, bazı risk analizleri uzun zamanlı ön çalıştırma gerektirirken, bazıları ise daha kalıplaşmış formlar uygulanarak kısa sürede sonuca varmayı sağlamaktadır.

Risk analizi ve yönetimi için geliştirilen yöntemlerin en uygun olanının seçimi, etkin risk yönetimi için önemlidir. Bu yöntemlerin hangisinin seçilip kullanılacağı bilgi güvenliği yöneticilerinin önemli bir problemidir. Risk analizi ve

yönetimi için geliştirilmiş birçok yöntem bulunmaktadır ve organizasyonlar bu yöntemlerden hangisini seçmeleri konusunda, objektif araçlara ihtiyaç duymaktadır. Bu nedenle, en uygun risk yönetim yöntemini seçmek için, organizasyona güven veren bir yaklaşım bulunmalıdır.

Bu çalışmada, bilgi güvenliği risk analizi ve yönetimi için seçilecek yöntemin belirlenmesi için bir yaklaşım önerilmiştir. Önerilen yöntem örnek bir vaka ile sınanarak elde edilen sonuçlar verilmiştir.

Makalenin devamında, bilgi güvenliği alanında risk analizi ve yönetimi ile ilgili temel bilgi ve literatürdeki ilgili çalışmalar verilmiştir. Bölüm 3'te önerilen risk analizi değerlendirme yöntemi anlatılmış, Bölüm 4'te uygulama sonuçları verilerek, sonuç bölümünde değerlendirme yapılmıştır.

2. Bilgi Sistemlerinde Risk Yönetimi

Bilgi sistemlerinde risk yönetimi iki temel ve bir yardımcı aktivite içerir. Risk değerlendirme ve risk indirgeme temel aktivitelerdir, belirsizlik analizi ise yardımcı aktivitedir [3].

2.1. Risk Değerlendirme

Risk değerlendirmenin ilk aşaması, risk yönetiminin en hayati, en uzun süren ve detaylı çalışması olan risk analizi işlemleridir. Risk değerlendirme işlemleri sırasında, risklerin tanımlanması, analizi, potansiyel etkilerinin belirlenmesi yapılır. Böylece bir sonraki adım olan risk indirgeme için, riski düşürücü stratejilerin önerilmesine yardımcı olunur. Risk değerlendirilirken, sistem üzerinde belirli zayıflıkların bulunması nedeniyle gerçekleşebilecek bir tehdidin oluşma olasılığının fonksiyonu olarak dikkate alınır. Bu zayıflıklar, mutlaka organizasyon üzerinde negatif etkilere sebep olabilecek nitelikte olmalıdırlar [4], [5].

Risk değerlendirmede öncelikle risk analizi yapılacak hedef alan ve sınırları belirlenir. Eğer varsa daha önceki analiz sonuçları da dikkate alınarak analiz edilecek sistemle ilgili varlık verileri toplanır (bu varlıklar; bilgi, yazılım, personel, donanım, fiziki varlıklar, vb. olabilir). Kayıp veya hasar açısından daha hayati kısımlara öncelik verilmesi amacıyla, önem derecelerine göre önceliklerinin belirlenmesi yapılır. Uygulanacak yöntem belirlenir. Risk hesaplaması yapılır. En son aşamada ise, organizasyon için nelerin önemli olduğunu yansıtabilecek anlamlı çıktılar oluşturularak, karar vericilere sunulmak üzere elde edilen sonuçlar dokümante edilir [3], [4].

2.1.1. Risk Analizi

Risk analizinde, gelecekte muhtemel olumsuz etkileri oluşturacak olaylar, tehditler, zayıflıklar, birbirleriyle etkileşimleri ve bunlara karşı önlem olarak düşünülebilecek koruyucular değerlendirilir. Burada sisteme yönelik olası olumsuz etkinin şiddeti, olayın kötü sonuçlarının ve etkilediği kaynakların değerinin fonksiyonudur. Öncelikle sisteme yönelik tehditler tanımlanarak analiz edilir, sisteme yönelik etkisinin daha önemsiz olabileceği düşünülenler veya organizasyon için hayati değer taşımayanlar elenir. Kalan tehditlerin gerçekleşmesine yol açan zayıflıklar analiz edilir. Tehdit-varlık-zayıflık ilişkilendirmeleri yapılarak seçilen yönteme göre risk hesaplanır. Riske karşı koruyucu önlemler ortaya konur. Son aşamada ise, bu koruyucuların maliyet/fayda açısından analizi gerçekleştirilir.

2.2. Risk İndirgeme

Risk indirgeme, karar vericiler tarafından riski kabul edilebilecek seviyeye indirgeyecek güvenlik kontrollerinin ve koruyucularının seçilmesi, bunların uygulanması ile ilgilidir [3]. Öncelikli olarak riski kabul edilebilir seviyeye getirmeyi hedefler. Bu amaçla risk koruyucu işlemleri ve koruyucuların maliyet-fayda analizleri gözden geçirilir. Sonuç olarak, riskle başa çıkma ve önlemler almada şu alternatifler düşünülür: riski olduğu gibi kabullenmek, riskten sakınmak, koruyucu kontroller uygulayarak riski önlemek, risk transferi [5], [6].

2.3. Belirsizlik Analizi

Riskin ana kaynağı belirsizliktir, belirsizlik yoksa risk de yoktur. Belirsizlik analizleri yapılır ve dokümante edilirse, risk yönetimi sonuçları bilgiye dayalı olacaktır. Risk yönetimi işlemlerinde belirsizliğin iki temel kaynağı vardır: (1) risk yönetim model veya yöntemindeki güven veya kesinlik eksikliği; (2) risk modeli elemanlarının (tehdit frekansı, koruyucu etkinliği ve sonuç gibi) tam değerlerini belirlemede yeterli bilgi eksikliği [3].

2.4. Risk Analizi Yöntemleri

Temel olarak, nitel ve nicel olmak üzere iki tür risk analizi metodolojisi vardır [7], [8] .Nitel metodolojilerde analiz, riski düşük, orta, yüksek şeklinde sıfatlar kullanarak sınıflandırmayla yapılır. Nicel metodolojilerde ise, matematiksel ve istatistiki ifadeler kullanılır ve sayısal değerler ortaya konur. Risk analizinde bu iki temel tür üzerinde geliştirilmiş çeşitli yöntemler kullanılır. Ayrıca bazı yöntemler, karma yapıdadır, yani iki yapıyı bir arada kullanmaktadır. Karma yapıdaki yöntemlerde bile, nitel veya nicel özelliklerden bir tanesi daha ağırlıklı olmakta, yöntem bu özelliğiyle daha nicel veya daha nitel olarak sınıflandırılabilmektedir. Kullandığı yöntem ister nitel, ister nicel olsun, genel olarak bütün risk analiz yöntemlerinin ana hedefi, toplam risk değerini tahmin etmektir.

2.5. Risk Yönetiminin Başarısı

Risk yönetim işlemleri sürekli bir yapıda olmalıdır. Yapılan işlemlerin periyodik olarak döngüsel tekrarlanmasıyla başarılı risk yönetimine ulaşılır. Zaman içerisinde yeni tehditler ve zayıflıklar ortaya çıkabilir. Aynı anda organizasyondaki kişiler veya sistemin yapısı değişebilir. Bu nedenle süregelen değişiklikler, risk yönetim görevlerinin düzenli aralıklarla yeniden değerlendirilmesini gerektirecektir [5].

3. Risk Analizi ve Yönetimi Yöntemi Seçimi ve Önerilen Yöntem

Bir organizasyon, kendi bilgi sistemlerine karşı mevcut tehditlerin riskini düşürebilmek için, birincil öncelikli olarak iyi bir risk yönetim programına ihtiyaç duyar. Organizasyon, kendi ihtiyaçlarını temel alarak kendisine en uygun risk analizi yöntemini seçmelidir. Bu amaçla zaman ve para harcanacağı için, uygulamadaki mevcut risk analizi yöntemlerini karşılaştırıp değerlendirerek kendi ihtiyaçlarıyla örtüşen bir yöntemi seçmesi kritiktir. Seçim için en iyi metod, bu yöntemlerin tarafsız ve nicel olarak karşılaştırılmasıdır [9].

3.1. Metodoloji Seçiminde Mevcut Yöntemler

En uygun risk analizi ve yönetimi seçimi için yapılan çalışmalar fazla sayıda değildir, dolayısıyla bu konu yeni araştırmalara açıktır. Bilgi güvenliği risk analizi yöntemlerinin karşılaştırmasını yapan eski çalışmalar, örneğin 1993 yılında Badenhorst'un çalışmasında da olduğu gibi, metodların organizasyonun ihtiyaçlarıyla ne şekilde örtüştüğünü anlamamızı sağlayan ölçekler kullanmak yerine; genellikle yöntemdeki bilgi teknolojileri, bilgi güvenliği ve risk yaklaşımının bazı kriterlere adreslenip adreslenmediğine odaklanırlar [9].

Yakın bir zamanda yapılan çalışma ise, Vorster'in farklı risk analizi metodolojilerini karşılaştırdığı çalışmadır. Bu çalışmada örnek olarak seçilen nitel ve nicel özellikli beş farklı metodoloji üzerinde inceleme yapılmıştır. Çalışmadaki karşılaştırma kriterleri şu şekildedir [9]:

- *Risk analizinin tekli varlıklar veya varlık grupları üzerinde yapılması:* Metodolojinin sonuçlarından tekli varlıklar ya da varlık grupları üzerinde yapıldığını anlayabiliriz. Varlıklar üzerinde tekil analiz yapılması, zaman açısından organizasyona maliyet getireceğinden organizasyonun yöntem seçiminde etkili olacaktır. Bu nedenle organizasyon çoğunlukla, varlık grupları üzerinde risk analizi gerçekleştirecektir.
- *Risk analizinin uygulandığı yöntemin bulunduğu yer:* Risk analizi için gereken bilgi ve çalışmaların miktarını belirleyen kriterdir. Yöntemde bu kriter, iki alternatifle değerlendirilir: (1) zaman, ya da daha kritik sistemler için (2) sonucun tamlığı. Bu kriter, organizasyonun önceliğine göre belirlenip ölçeklendirilebilir.
- *Risk analizine katılan kişiler:* Analizin, organizasyonun dahilindeki kişilerle veya harici kişilerin katılımıyla olması maliyet ve uzmanlık açısından farklılık yaratacaktır. Burada da kriter olarak organizasyonun maliyet veya uzmanlık önceliğine göre ölçekleme yapılmasına imkan sağlanmıştır
- *Kullanılan ana formül:* Uygulanan yöntemdeki matematiksel formülün karmaşıklığı, zaman ve sonucun güvenilirliği açısından değerlendirilir. Organizasyon isteğe bağlı olarak bu kriteri kolaylık ve sonucun tamlığı seçeneklerinden birini gözönüne alarak değerlendirebilir.
- *Sonuçların bağıl ya da mutlak olması*: Uygulanan yöntem sonucu bulunan sonuçlar, her zaman karşılaştırılabilir olmayabilir. Örneğin, bir yöntemde iki varlığa yönelik bulunan risk sonucu da yüksek ise, hangisinin daha büyük risk taşıdığını söylemek mümkün olmayacaktır. Ama başka bir yöntemde bulunan iki risk değeri 200 ve 100 ise, birincinin ikinciye göre daha yüksek risk taşıdığını söylemek mümkündür.

Vorster, analiz ettiği yöntemleri bu kriterler bazında değerlendirmiş, ölçeklendirmiş ve karşılaştırma için bir tablo oluşturmuştur. Yöntem, beş kriterden her birinin önem derecesine bağlı olarak, organizasyon tarafından ağırlık katsayısı seçilmesini olanaklı kılmıştır. Her bir yöntem için; kriterlerin değeri, bu ağırlık katsayısıyla çarpılıp toplandığında o yöntem için bir değer bulunacaktır. En büyük değeri olan yöntem, organizasyonun ihtiyaçlarıyla en iyi örtüşen yöntem olarak değerlendirilir.

Bu çalışma farklı özelliklerdeki risk analiz yöntemlerine uygulanabileceği ve organizasyonun ihtiyaçları doğrultusunda katsayılarla şekillendirilebileceği için olumlu bir tablo çizmesine rağmen, Vorster'in makalesinde de belirttiği gibi bazı zayıflıklara sahiptir. Örneğin, makale ile belirlenen kriterler haricinde en uygun yöntem seçiminde etkin olabilecek farklı kriterler de bulunabilir. Seçenekli hale getirilmiş bazı kriterler, uygulayıcıları iki özellikten birini seçmeye zorlamaktadır. Organizasyonun ihtiyaçlarını tatmin için sadece ağırlık katsayılarının kullanılması yeterli olmayacağı gibi, bu katsayıların belirlenmesi de net değildir.

3.2. Metodoloji Seçimi İçin Önerilen Yöntem

Çalışmaya başlarken temel alınan nokta, birçok risk analizi ve yönetimi yöntemi olmasına karşın bunların genel anlamda birbirlerine üstünlüklerinin olmadığı, ancak uygulayan organizasyonun ihtiyaçları çerçevesinde o organizasyon için en iyi olan yöntemin bulunması gerekliliği sonucudur.

3.2.1. Önerilen Yaklaşımın Detayları

Herhangi bir organizasyon için ihtiyacın belirlenmesinde risk analizi ve yönetimiyle ilgili bazı nitelikleri düşünmek gerekmektedir. Bunlar, gerek organizasyon, gerekse yöntem için evet/hayır cevaplı sorulara dönüştürülebilirler. Aşağıda bu nitelikler ve bunlara göre tasarlanmış sorular listelenmiştir:

S.1. Varlıkların önem dereceleri:

Organizasyon için: Sistemin herhangi bir parçasındaki bir aksaklık, diğer parçaları da etkileyebilir mi?

Yöntem için: Varlıklar tekil olarak değil de grup olarak mı değerlendiriliyor?

S.2. Maliyet:

Organizasyon için: Maliyeti düşük olmalı mı?

Yöntem için: Maliyeti düşük mü?

S.3. Sonuçların kesinliği:

Organizasyon için: Genel durum analizindense, net sonuçlara mı ihtiyaç var?

Yöntem için: Riskler hakkında genel bir çalışma niteliğinden çok, net sonuçlar ortaya koyabiliyor mu?

S.4. Uygulanacak yöntemde kullanılan malzeme:

Organizasyon için: Kendi sorularını kendisi tasarlamak yerine, hazır sorular, testler şeklinde bir yapıya mı ihtiyaç duyuluyor?

Yöntem için: Uygulamada kullanıma hazır şablonlar mevcut mu?

S.5. Yöntemin güncellenebilir olması:

Organizasyonun için: Güncellenebilir bir yönteme tercih eder mi?

Yöntem için: Yöntem güncellenebilir mi?

S.6. Uygulayıcılar:

Organizasyon için: Analizler için organizasyon dışından şahıslar tercih edilir mi?

Yöntem için: Organizasyon dışından teknik uygulayıcılara ihtiyaç var mı?

S.7. *Yöntemin sonucunun nitel veya nicel olması*

Organizasyon için: Tercih edilen metrik nicel midir?

Yöntem için: Uygulanan metrik nicel midir?

S.8. *Yöntemin sektör için kullanılabilirliği veya adapte edilebilirliği*

Organizasyon için: (Evet)

Yöntem için: Organizasyon yöntemin uygulanabileceği sektörlerden midir?

S.9. *Yöntemin uç durumlara uygulanabilirliği*

Organizasyon için: Organizasyonda analiz edilmesi gereken uç durumlar var mı?

Yöntem için: Yöntem en uç durumları analiz edebilecek yapıda mıdır?

S.10. *Yöntemin koruyucu seçimindeki durumu*

Organizasyon için: Koruyucu seçimi için önerilere ihtiyaç duyuluyor mu?

Yöntem için: Koruyucu öneri modülü mevcut mu?

S.11. *Yöntemin raporlama durumu*

Organizasyon için: Detaylı raporlara ihtiyaç var mı?

Yöntem için: Detaylı raporlama modülü mevcut mu?

S.12. *Yöntemin uygulanma zamanı*

Organizasyon için: Uygulanması kısa süre gerektiren bir uygulamaya mı ihtiyaç var?

Yöntem için: Yöntemin uygulanma süresi kısa mı?

S.13. *Yöntemin bakımı (satın alınma sonrası destek gerekliliği)*

Organizasyon için: Organizasyon bakım gerektiren bir yöntemi kullanabilir mi?

Yöntem için: Yöntemin bakıma ihtiyacı var mı?

S.14. *Yöntemin sonuçları*

Organizasyon için: Organizasyon yöntem sonuçlarının aynı birimden, dolayısıyla karşılaştırılabilir olmasını mı istiyor?

Yöntem için: Yöntemin sonuçları aynı birimden ve karşılaştırılabilir mi?

Tüm bu listenen ve benzer şekilde eklenebilecek nitelikler, evet/hayır cevaplı sorulara dönüştürülebilir. Ya da uygun metodoloji seçimi çalışması öncesi, burada listelenen sorulardan istenilenleri değerlendirme dışı bırakılabilir.

Seçim için kritik olduğu düşünülen niteliklere ait sorular, organizasyon tarafından ihtiyaçları doğrultusunda sırayla evet veya hayır değerleri ile değerlendirilir. Evet cevapları 1 ile, hayır cevapları 0 ile temsil edilirler. Dolayısıyla, toplam soru sayısı n ve $i = 1, \ldots n$ için, S_i 'ler de her bir niteliği karakterize eden organizasyon tarafındaki sorular olmak üzere, S_i'ler 1 veya 0 şeklinde değerler alabilirler.

Diğer bir taraftan ise, organizasyon için değerlendirilen tüm nitelikler için aynı sırada olmak üzere, incelenmek istenilen k nolu yöntem, evet/hayır cevaplı sorularla değerlendirilir. Benzer şekilde evet cevapları 1 ile, hayır cevapları 0 ile belirlenir. Dolayısıyla, değerlendirilen soruların toplam sayısı yine n olacağından, $i = 1, \ldots n$ için M_i 'ler her bir niteliği karakterize eden yöntem tarafındaki sorular olmak üzere, M_{ki}'ler 1 veya 0 şeklinde değerler alabilirler.

Organizasyon için uygun metodolojiyi belirlemek amacıyla, incelenen m yötemin her biri için, $k = 1, \ldots m$ olmak üzere, k yönteminin uygunluğu:

$$TM_k = \sum_i^n (S_i \Leftrightarrow M_{ki}) \quad (1)$$

değeri ile hesaplanır. En büyük TM_k değerini veren yöntem, organizasyona en uygun ve önerilen yöntemdir.

4. Örnek Uygulama ve elde edilen sonuçlar

Örnek organizasyonumuz, bilgi güvenliği için dört alternatif risk yönetim yönteminden kendi ihtiyaçlarına en iyi cevap verebilecek olanını seçmek istiyor. Bu alternatif yöntemler, sırasıyla, CRAMM, CORAS, ISRAM ve OCTAVE'dır.

4.1. Y1: CRAMM (CCTA Risk Analysis and Management Methodology)

BS7799'la tam uyumlu ve ayrıntılı risk değerleme araçlarından oluşur. Organizasyonun varlıklarını, işlemlerini, uygulamalarını, sistemlerini, tehdit ve zayıflıklarını, risk seviyelerini, koruyucuları; güvenlik yönünden analiz etmek için sorular kullanır. Potansiyel problemleri dikkate alarak nitel analiz yapar. Kullanıcının verdiği yanıtlar doğrultusunda koruyucuları değerlendirerek birbirlerine göre önceliklerini belirler, koruyucu maliyetlerini tahminler, güvenlik politikası geliştirilmesine yardımcı olur ve denetleme yapılmasını olanaklı kılar [10].

Varlık tanımlama ve değerleme, tehdit ve zayıflık değerlendirmesi, öneriler ve karşı önlemler şeklinde üç adımdan oluşur. Öneriler ve karşı önlemler adımında detaylı koruyucu kütüphanesi kullanılır. CRAMM yazılımı, belirlediği risk değeri ve istenen bir güvenlik eşiği değeri için bu koruyucuları karşılaştırarak karar verilmesini kolaylaştırır [10].

4.2. Y2: CORAS (Construct a platform for Risk Analysis of Security Critical Systems)

CORAS, nitel risk analizi yöntemini kullanır. Temel amaçlarından biri risk analizi için yöntemler, nesneye dayalı modelleme için yarı formal yöntemler, güvenliğin kritik olduğu sistemlerde kesin, belirgin ve etkin bir risk analizi sağlayan kompüterize araçları sınayan bir çerçeve geliştirmektir [9]. Varlıklar, tehditler ve zayıflıklar arasındaki ilişkileri ve riskin bulunduğu ortam arasındaki bağlantıları göstermek için görsel diyagramlar (UML) kullanılır. Risk analizi sırasında toplanan bilginin çoğu, beyinfırtınası, seminer ve tartışmalarla, farklı alanlar ve düzeylerde uzman olan kişilerin bir araya gelmesi ve fikirlerin, bilgilerin paylaşılmasıyla ortaya konur. Uygulanan işlemler açısından, biri risk yönetimi olmak üzere dört ana aşamadan ve toplam yedi adımdan oluşur. Final sonuç, her bir varlık için farklı UML sınıfı diyagramı şeklindedir ve bu görsel diyagramlarda, varlıklar için söz konusu tüm kaynakları, mevcut riskleri, birbirleriyle olan etkileşimlerini ve bu şekilde riskin derecesini nitel sıfatlarla görmek mümkündür [9], [11].

4.3. Y3: ISRAM (Information Security Risk Analysis Method)

Organizasyondaki yönetici ve diğer personelin bir arada yaptıkları tetkik çalışmaları ile gerçekleşen nicel ve doküman temelli bir risk analizi yöntemidir. En önemli adımında riski tetikleyen olasılıklar ve sonuçlarla ilgili tüm faktörler belirlenerek listelenir, faktörlere ağırlık değerleri atanır ve iki ayrı tetkik testine dönüştürülür. Bu testlerin amacı, bilgi güvenliği probleminin organizasyondaki olumsuz etkilerini ve derecelerini ortaya koymaktır. Testler uygulandıktan sonra, sonuçları ISRAM için şekillendirilmiş risk formülüne uygulanır. Böylece sonuçta tek bir sayısal değer elde edilir. Son aşamada ise elde edilen sayısal değer ve testlerdeki soruların cevapları da analiz edilerek değerlendirilir [7], [9].

4.4. Y4: OCTAVE

Varlıklar, tehditler ve zayıflıklara odaklanan ve risk değerlemeyi organizasyon dahilindeki kişilerin idare etmesini öngören bir yöntemdir. Riski hesaplarken nitel kriterler kullanır. Uygulanması şart olan belirli aktiviteleri işlemlerini içeren üç fazdan oluşur. Risk kararı için elde edilen sonuçları, her bir varlık için tehdit profiline dayanır [9].

4.5. Yöntemimin Uygulanması

Bölüm 3.2'de önerilen yöntem organizasyonun yöntem seçimi için uygulanmıştır. 3.2.1'deki on dört soru sırasıyla organizasyona ve alternatif yöntemlere göre cevaplandırıldığında elde edilen sonuçlar, Tablo 1'de verilmiştir.

Tablo 1: Uygulama Sonuçları

Soru	Org	Y1	Y2	Y3	Y4	Y1 ⇔ Org	Y2 ⇔ Org	Y3 ⇔ Org	Y4 ⇔ Org
S.1	1	0	0	1	0	0	0	1	0
S.2	1	0	1	1	1	0	1	1	1
S.3	0	1	0	1	0	0	1	0	1
S.4	1	1	0	0	0	1	0	0	0
S.5	0	1	0	0	0	0	1	1	1
S.6	0	0	0	0	0	1	1	1	1
S.7	1	1	0	1	0	1	0	1	0
S.8	1	1	1	1	1	1	1	1	1
S.9	0	1	1	1	1	0	0	0	0
S.10	0	1	0	0	0	0	1	1	1
S.11	0	1	0	0	0	0	1	1	1
S.12	1	1	0	0	0	1	0	0	0
S.13	0	1	0	0	0	0	1	1	1
S.14	1	1	0	0	0	1	0	0	0

Bu durumda yöntemlerin uygunlukları, (1) formülü dolayısıyla $TM_1 = 6$, $TM_2 = 8$, $TM_3 = 9$ ve $TM_4 = 8$ şeklinde olacaktır. Dolayısıyla, örnek organizasyonun risk yönetiminde kullanması için üçüncü alternatif olan ISRAM yöntemi daha uygundur.

5. Sonuç ve Öneriler

Günümüzde organizasyonlar, bilgi güvenliğini sağlamak için risk yönetiminin öneminin ve uzman bir yöntem kulllanımının gerekliliğinin farkındalar. Bu çalışmada, söz konusu problem için bir model önerilerek test edilmiştir.

Önerilen model, organizasyonun yapısını ve beklentilerini ortaya koyacak şekilde bu yaklaşımı tespit etmektedir. Bu amaçla hazırlanan sorular cevaplandığında, organizasyonun ihtiyaçları ve öncelikleri belirlenirken, risk analizine olan güvenin de güçlenmesi sağlanacaktır.

Soruların yöntemleri analiz eden karşılıklarıyla da, istenilen sayıdaki uygulanması düşünülen yöntem, tarafsız olarak değerlendirilebilir. Organizasyonun ihtiyaçlarına en uygun risk analizi yöntemi, modelde tanımlanan ve uygulanması pratik olan uygunluk formülü yardımıyla tespit edilebilir.

Yeni bir risk analiz yöntemi, organizasyon için değerlendirilmek istendiğinde, organizasyonun ihtiyaçları değişmemişse, sadece bu yöntem için sorular yardımıyla yeni bir değerlendirme yapılır ve yöntemin uygunluğu hesaplanır. Elde edilen sonuç, daha önceki yöntemlerin uygunluk değerleri ile karşılaştırılarak yeni yöntemin organizasyon için daha iyi olup olmadığı belirlenir. Ayrıca organizasyonun ihtiyaçları değiştiği takdirde, sadece organizasyon için değerlendirme soruları tekrar uygulanarak, tüm yöntemler tekrar sorularla analiz edilmeden, sadece yöntemlerin uygunluk değerleri güncellenir ve karşılaştırma yapılabilir.

Kaynaklar

[1] ISO/IEC 17799 International Standard, Information technology – Code of pactice for information security management, Switzerland, 2000.

[2] Aime, M. D., Atzeni A., Pomi, P. C., "AMBRA: Automated Model-based Risk Analysis", *QoP '07: ACM workshop on Quality of protection*, 2007.

[3] Swanson, M., Guttman, B., "Generally Accepted Principles and Practices for Securing Information Technology Systems", *NIST Special Publication 800-14,* 1996.

[4] NIST, "An Introduction to Computer Security: The NIST Handbook", *NIST Special Publication 800-12.*

[5] Dhillon, G. (Repasky, N.), *Principles of Information System Security*, Wiley, USA, 2007.

[6] Blakley, B., McDermott, E., Geer, D., "Information security is information risk management", *NSPW '01: Proceedings of the 2001 workshop on New security paradigms*, 2001.

[7] Karabacak, B., Sogukpinar, I., "ISRAM: Information Security Risk Analysis Method", *Computers & Security*, 24(2), 147-129, 2004.

[8] Bella, G., Bistarelli, S., Peretti, P., Riccobene, S., "Augmented Risk Analysis", *Electronic Notes in Theoretical Computer Science*, Volume 168, Pages 207-220, 2007.

[9] Vorster, A., Labuschagne, L., "A framework for comparing different information security risk analysis methodologies", *Proceedings of the 2005 annual research conference of the SAICSIT '05*, 2005.

[10] UK Central Computer and Telecommunication Agency (CCTA), Risk Analysis and Management Method, *CRAMM User Guide*, Issue 2.0, 2001.

[11] Braber, F., Hogganvik, I., Lund, M.S., Stolen, K., Vraalsen, F., "Model-based security analysis in seven steps - A guided tour to the CORAS method", *BT Technology Journal*, v 25, n 1, p 101-117, 2007.