Bilgi Güvenliği Risklerinin Değerlendirilmesinde Yeni Nesil Yöntem: OCTAVE Allegro

A New Generation Method for Assessing Information Security Risks: OCTAVE Allegro

Dr. Emine Serap Kurt 0000-0003-2192-0669
Research assistant Aysu Yaşar 0000-0003-2200-2915
Assoc. Prof. Dr. Kenan Terzioğlu 0000-0002-6053-830X
Dr. Senem Demirkıran 0000-0001-9835-4963

Abstract

Information system risk assessment, an essential aspect of information security management, assists organizations in identifying and analyzing critical information system assets and reducing potential risks. Internal control and risk management are two systems that complement each other in controlling an organization's activities. As a result, internal control activities, critical for controlling and managing risks, should be carried out with a risk focus. Institutions should first analyze the risks that may emerge in business processes before evaluating the steps that should be taken to secure their information assets. Many risk assessment methods are complicated and expensive, and qualified professionals should only carry them out. The OCTAVE Allegro method is a comprehensive assessment of an organization's operational risk environment to get better results without requiring considerable risk assessment information. Risk assessment can be completed in a short period and at a low cost using this method, and the effectiveness of internal control can be improved. The study's objective is to give information about the OCTAVE Allegro method, which can help prevent the risks of ensuring information security as information technologies advance and explain the method's application areas.

1 Giriş

Bilgi sistemi, bir kuruluş içindeki günlük işlem işleme ihtiyaçlarını uzlaştıran, bir kuruluşun operasyonunu, yönetimsel ve stratejik faaliyetlerini destekleyen ve belirli dış taraflara gerekli raporları sağlayan bir sistemdir. Bilgi sistemleri, bir organizasyonda karar verme, koordinasyon, kontrol, problem analizi ve görselleştirmeyi desteklemek için bilgileri toplamak, işlemek, depolamak ve yaymak için birlikte çalışan bileşenlerdir (Suroso and Fakhrozi, 2018). Bilgisayar tabanlı bilgi sistemlerindeki hızlı gelişmelerle dijital verileri işlemek, depolamak ve iletmek; kamu hizmeti, ticaret, sağlık ve eğitim vb. çoğu sektörde avantaj sunmaktadır. Bu avantajların yanı sıra bilgi iletişim teknolojilerinde yaşanan değişiklikler kurumsal açıdan paydaşlar arasında bilgi sistemlerinin güvenliğiyle ilgili endişeleri ortaya çıkarmaktadır. Sağlam bir iç kontrol sistemi, dolandırıcılığına karşı en güçlü savunma olsa da kuruluşlar olası dolandırıcılık eylemlerini caydıracak uygun yapıların ve kültürün oluşturulması konusunda da çalışmalıdır (Zekıć and Mılıć, 2016). Kuruluşlar için artık bilginin korunması, teknik sorunları çözmekten daha önemli olmaktadır (Dhillon ve Backhouse, 2000). Güvenlik endişeleri, kamu sektöründe ve özel sektörde bilgi güvenliği sistemlerini geliştirerek bu sistemlerin kullanımını arttırmaktadır. Güvenlik sorunlarından kaynaklanacak bilgi güvenliği risklerini azaltmak için yüzlerce bilgi sistemi risk yönetimi yöntemi ve standardı bulunmaktadır. Fakat güvenlik risklerinin fazlalığı nedeniyle hepsine karşı önlemler geliştirilmesi kuruluşlar için maliyetlidir (Dubois vd., 2010). Bilgi ve iletişim teknolojilerinin kamu sektörünün ve özel sektörün tüm alanlarında kullanılması devletin ve vatandaşların bilgi sistemlerine bağımlı hale gelmesine ve bilgi sistemleri güvenliğinin önemli hale gelmesine neden olmaktadır (Prieß ve Hoppe, 2005). Uygun güvenlik önlemlerinin seçiminde sorunun çeşitli boyutları ve bunların birbirleri ile ilişkileri dikkate alınması gerektiğinden kuruluşlar için ticari bir varlık önemi taşıyan bilginin uygun şekilde korunması özellikle giderek artan tehditlere ve güvenlik açıklarına maruz kalındığı iş ortamında önemli olmaktadır. Bilginin korunmasına yönelik bilgi işleme/depolama için kullanılan ekipman ve prosedürlerin risk değerlendirmesi yapılarak, bilgi güvenliğindeki güvenlik açıklarından kaynaklanacak firma itibar kayıplarının veya finansal kayıpların önüne geçilmektedir.

Bilgi sistemi uygulamalarının kullanımında bilgi güvenliğiyle verilerin saklanması ve kullanılması sürecinde bilginin gizliliğini, bütünlüğünü ve kullanılabilirliğini etkileyebilecek tehditlerin ve olası saldırıların önüne geçilmesi amaçlanmaktadır. Bilgi sistemlerinin güvenliği sadece güvenlik araçlarına/ teknolojisine dayanmamakta aynı zamanda kuruluşların koruması gereken araç veya varlıklarının bilgi güvenliği sorunlarını ortadan kaldıracak olan uygun çözümlerin belirlenmesini de gerektirmektedir. Bu nedenle, sistematik ve kapsamlı bir bilgi güvenliği yönetimine ihtiyaç duyulmaktadır. Bazı kuruluşlar, güvenlik riski yönetimi bilgilerini desteklemek için OCTAVE yöntemini kullanmakta ancak yöntemin uygulama adımlarının karmaşıklığı göz önüne alındığında uygulamanın benimsenmesinin zor olduğu görülmektedir. OCTAVE ve diğer geliştirilen alternatiflerinin uygulanmasında bazı gereksinimler bulunmakta ve bu gereksinimler değerlendirilmesi yapılacak olanın ne olduğunu tespit etmeye ve değerlendirme sebebini tanımlamaya yardımcı olmanın yanı sıra faaliyetin başarılı olup olmadığını ölçmenin bir

yolunu da sağlamaktadır. OCTAVE'nin uygulanmasında, öğretilmesinde ve kullanımında elde edilen deneyimler daha bilgi merkezli bir risk değerlendirmesine geçilme ihtiyacını ortaya koymaktadır. Bilgi varlıkları, bilgi güvenliği değerlendirmesinin odak noktası olduğunda diğer tüm varlıklar, bilgi varlıklarının depolandığı, taşındığı ve işlendiği alanlar olarak değerlendirme sürecine dahil edilebilmektedir. Depo olarak nitelendirilen alan, bir kişi, nesne (örneğin bir kâğıt parçası) veya bir teknoloji (örneğin bir veri tabanı) olabilmekte ve bilgi varlıklarına yönelik tehditler, muhafaza edildiği konum belirlenerek incelenmektedir. Böylelikle sürece dahil edilen varlıkların sayısı ve türleri sınırlandırılmakta ve bu durum bilgi varlıklarına odaklanmak ve risk değerlendirmesi yapmak için toplanması, işlenmesi, düzenlenmesi, analiz edilmesi ve anlaşılması gereken bilgi miktarını etkin bir şekilde sınırlamaktadır.

Güncellenmiş bir OCTAVE yaklaşımı geliştirmenin adımları (saha kullanımı, gözlem ve sınıf deneyiminden elde edilen); kullanım kolaylığının sağlanması, değerlendirme kapsamının tanımının iyileştirilmesi, eğitim ve bilgi gereksinimlerinin azaltılması, kaynak taahhütlerinin azaltılması, kurumsallaşmanın ve tekrarlanabilirliğin teşvik edilmesi, kurum genelinde tutarlı ve karşılaştırılabilir sonuçlar üretilmesi, risk değerlendirmesi temel yetkinliğinin geliştirilmesi, kurumsal uyumluluk gereksinimlerinin desteklemesi şeklinde sıralanabilir. Bu çalışma, Trakya Üniversitesi tarafından desteklenen 2021/133 proje numarasına sahip "E-Devlet Bilgi Güvenliği Risk Değerlendirmesi: Yapay Sınır Ağ Modellemesi" adlı bilimsel araştırma projesi kapsamında incelenmektedir.

2 Kavramsal Çerçeve

Bilgi ve iletişim teknolojilerinin (BİT) gelişmesi ve internete erişimin artmasıyla birlikte kuruluşlar siber saldırılar başta olmak üzere çalışanların faaliyetleri veya bilgisayar korsanlarının saldırıları gibi mali kayıplara neden olan çeşitli tehdit türlerine karşı savunmasız hale gelmektedir. Bilgi sistemleri, bir kuruluş için bilgi işleme; bilgi edinme, kaydetme, depolama, iletme, dönüştürme ve sağlama yapan sosyo-teknik iş sistemleridir. Donanım ve yazılımdan oluşan teknik bileşenler ile organizasyonel düzenlemeler ve kavramlar, çalışanlardan oluşan kullanıcılar ve denetçiler/sorumlular vb. teknik olmayan bileşenlerden oluşmaktadır. Bu bileşenlere ek olarak bilgi sistemi altyapısının ve bilgi sistemi yönetimi yazılımının parçası olmayan; servis personeli, tedarikçiler, müşteriler, bilgisayar korsanları vb. kişiler bilgi sistemi güvenliği için tehlikelerin ve güvenlik açıklarının başlangıç noktaları veya nedenleridir. Bilgi sistemlerinden bağımsız olarak meydana gelen hasarların nesnel olasılıklarını ifade eden tehlikeler, bilgi sistemi bileşenlerine zarar vermeyi, bu bileşenleri değiştirmeyi veya yok etmeyi içeren saldırılar olabilmekte ve bilgi sistemi güvenliğine hizmet eden tüm faaliyetleri içeren uygun bir güvenlik önlemi ile engellenmezse güvenlik açığı söz konusu olmaktadır (Jouini vd., 2014).

Tehlike ve zararlardan korunma durumunu tanımlayan güvenlik kavramı, veri güvenliği, iletişim güvenliği ve bilgi güvenliği gibi incelenen nesneye bağlı olarak belirli bir odakla incelenmektedir. Sosyo-teknik bilgi sistemlerinde güvenlik kavramının tüm yönleri bir arada düşünülerek bütünleştirilmelidir. Bilgi sistemleri güvenliği; *gizlilik, bütünlük, doğruluk/güvenilirlik* ve *yetki* başta olmak üzere pek çok farklı yönü içermektedir (Prieß ve Hoppe, 2004; Sukri and Riadi, 2021). *Gizlilik*, veri ve mesaj alışverişi sırasındaki temel sorundur ve veriler sadece yetkili kişilerin erişimine açık olmalıdır. Gizlilik için kriptografik şifreleme yöntemleri kullanılmaktadır. *Bütünlük*, gizliliğe bakılmadan değiş tokuş edilen veya depolanan verilerin bütünlüğünü ifade etmektedir. *Doğruluk/güvenilirlik*, şifre tabanlı girişler, biyometrik sistemler ve dijital imza vb. ile kimlik doğrulamayı içermektedir. Bir kişinin gerçekten olduğunu iddia ettiği kişi olduğuna dair kanıt sunmadır. *Yetki* ise sadece kimliği doğrulanmış kullanıcının izin veya yetkisine sahip olduğu verilere erişebilmesinin garanti edilmesidir (Kuhlen ve Semar, 2013).

Li ve Li (2018)'e göre, küreselleşmenin zorlukları ve fırsatları nedeniyle bilgi güvenliği, bilginin bütünlüğü, uygulanabilirliği ve gizliliği için hayati önem taşımaktadır. Li, Al-Shawabkeh ve Li (2018), bilgi güvenliği yönetim sistemini uygulama konusunda stratejik bir karar alacak kuruluşu etkileyen önemli nedenlerin kuruluş amaçları, güvenlik gereksinimleri, kuruluş boyutu, süreçleri ve yapısı olduğunu ifade etmektedir. Koduah ve Buchanan (2018), bilgi güvenliği değerlendirmesinin temel amacının organizasyonel operasyonlara yönelik riskleri belirlemek, tahmin etmek ve önceliklendirmek olduğunu ileri sürmektedir. Ak ve Gül (2019) 'a göre bilgi güvenliği gizlilik, bütünlük ve erişilebilirlik ana unsurlarının birleşimi ve bilgilerin başkasına aktarılmamasıdır. Bu üç güvenlik unsurundan biri zarar gördüğünde güvenlik zafiyeti oluşmakta ve kuruluşların bilgiye olan bağımlılığı bilgi güvenliği risk değerlendirmesini gerekli kılmaktadır. Matulevi˘cius ve Savukynas (2019), bilgi güvenliği risk yönetimini, fiziksel nesnelerdeki kullanıcılar ve gömülü sensörler tarafından oluşturulan veri ve bilgileri değiş tokuş etmek veya biriktirmek için bağlı cihaz ve sistemlerden oluşan bir ağ olan Nesnelerin İnterneti (IoT) sistemlerinde uygulayarak, verilerin çeşitli cihazlar ve birden çok kullanıcı arasında gönderilmesinde güvenliğin önemli bir rol oynadığını ifade etmekte ve bilgi güvenliğini tanımlamaktadır. Chen ve Zhu (2019)'a göre siber ağlarda kullanıcıların bilgi güvenliği yönetimleri ve uygulamaları en zayıf halka olarak görüldüğünden bilgi güvenliği sistemlerini merkezi olmayan bir şekilde güçlendirmek çok önemlidir.

Leonard vd. (2020) bilgi güvenliği kavramının donanım, veri, yazılım, altyapı ve bilgilerin yetkisiz kişiler tarafından kötüye kullanılmasına karşı korunması için kullanıldığını ve bilgi güvenliği tehditlerinin ise şirket bilgi kaynaklarını tehlikeye atma potansiyeline sahip kişiler, kuruluşlar, mekanizmalar veya olaylar olduğunu, bunun

yanı sıra sistematik bir iş riski yaklaşımına dayalı olarak bilgilerin korunması ve yönetilmesi, bilgi güvenliğinin oluşturulması, uygulanması, işletilmesi, izlenmesi, gözden geçirilmesi, sürdürülmesi ve iyileştirilmesinin bir yolu olan bilgi güvenliği yönetim sisteminin amacının veri ve bilgilerin değişimi, işlenmesi, depolanması, trafiği ve imha edilmesinden kaynaklanan risk düzeyini en aza indirmek olduğunu ifade etmektedir. Szczepaniuk vd. (2020) bilgi güvenliği kavramını kamu yönetimi çerçevesinde incelemekte ve kamu kurumlarının her düzeydeki faaliyetlerinde idari süreçlerin gerçekleştirilmesini ve bilgi güvenliğinin sağlanabilmesini kamu yönetiminde bilgi güvenliği olarak tanımlamakta ve kamu yönetiminde bilgi güvenliğinin bir durum ve süreç olarak tanımlanmasını önermektedir. Wang (2021), bilginin artan açıklığının bazı kişi veya kuruluşlar tarafından art niyetle yasadışı amaçlarla kolayca kullanılabildiğini ve bu nedenle ülkeler, işletmeler ve bireyler için bilgi sistemi güvenliğinin geliştirilmesinin gerekliliğini ifade etmektedir. Kuzminykh vd. (2021), bir varlığın veya varlık grubunun güvenlik açıklarını kuruluşa zarar vermek için belirli bir tehdit olarak kullanma olasılığını bilgi güvenliği riski olarak tanımlamaktadır. Wei ve Yao (2021), ağ bilgilerinin kurumsal çalışmalarda önemli rol oynadığını fakat güvenlik riskleri ile karşı karşıya olduğunu, ağın açıklığının ve paylaşımının ağ güvenliğini ve bilgi sistemini tehdit ettiğini ifade etmektedir. Kokkonda (2022)'ye göre, bilgi güvenliği sistemleri tehditleri ile ilgili çalışmalar ve analizler karmaşıklık ve IoT cihazlarının heterojen doğası nedeniyle yetersizdir. Rahmani vd. (2022), bilgi güvenliği sistemlerinde kullanıcı verilerini korumak için kurallar ve düzenlemeler geliştirildiğini fakat kullanıcılarla ilgili bilgilerin IoT ile eşleştirildiğinde toplanan verilerin yakalandığını ve bunun da veri güvenliği için kurallar, düzenlemeler ve politikalarda başarısızlığa yol açtığını, bu nedenle IoT'nin siber güvenlik tehdidini anlamak için mücadele ettiğini ifade etmektedir. Aleuatdinovich ve Usarovna (2022) ise bilgi güvenliği sisteminin kuruluşun yönetiminin ayrılmaz bir parçası olduğunu, bilgi güvenliğini sağlamak için riskleri doğru bir şekilde değerlendirmenin ve gerekli sistem güvenliği özelliklerinin tanıtılmasının önemi üzerinde durmaktadır. Bir kuruluşta bilgi güvenliği sürecini uygulama görevi; kuruluş düzeyi, teknik ekipman geliştirme düzeyi, gizlilik politikası, bütünlük sorunları, kullanılabilirlik ve süreklilikte bilgi sistemi güvenliğinin sağlanarak sistem ve uygulama önlemlerinin iyileştirilmesidir.

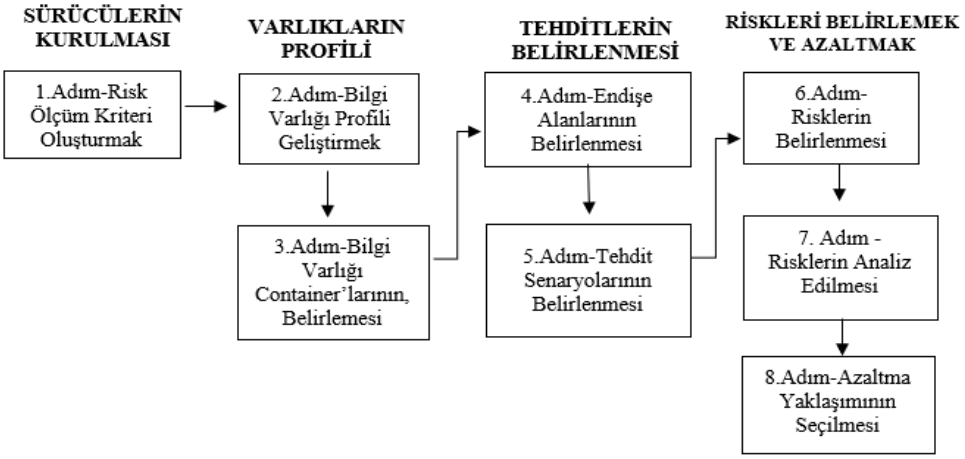
3 OCTAVE Allegro

Operasyonel Olarak Kritik Tehdit, Varlık ve Güvenlik Açığı Değerlendirmesi (Operationally Critical Threat, Asset, and Vulnerability Evaluation-OCTAVE), bir kuruluş içindeki bilgilerin tanımlanması ve yönetimi için Carnegie Mellon Üniversitesi'ndeki Yazılım Mühendisliği Enstitüsü (Software Engineering Institute-SEI) tarafından geliştirilen bir metodolojidir. Bu yönteme göre, tüm analiz süreci, dış danışmanların katılımı olmadan, kendi kendini yöneten bir yaklaşım izlenerek kuruluşun personeli tarafından gerçekleştirilmektedir (Kuzminykh vd., 2021). OCTAVE yöntemi, çok katmanlı hiyerarşiye sahip, kendi bilgi işlem altyapısını sürdüren, güvenlik açığı değerlendirme araçlarını çalıştırabilen kuruluşlar için geliştirilmiş olup bu kuruluşlarca uyarlanabilecek bir yapıya sahiptir. Kuruluşlar, OCTAVE yöntemini kullanarak gizlilik, bütünlük ve kullanılabilirliği dikkate alarak kritik bilgi teknolojisi varlıklarının korunmasına yönelik stratejiler geliştirebilmektedir. Yeni nesil OCTAVE yaklaşımı olan OCTAVE Allegro yöntemi de kuruluşların misyonlarını yerine getirmek için güvendikleri stratejik etkenler kapsamında bilgi güvenliği risk değerlendirmelerini yapmalarına yardımcı olmak üzere geliştirilmektedir. OCTAVE Allegro tarafından ulaşılacak hedefler, risk değerlendirmesi açısından kapsamlı bilgiye ihtiyaç duymadan daha iyi sonuçlar üretmek amacıyla bir kuruluşun operasyonel risk ortamının kapsamlı bir değerlendirmesidir (Suroso and Fakhrozi, 2018). OCTAVE Allegro, diğer OCTAVE yaklaşımlarından farklı olarak varlıkların kullanım, depolanma, aktarılma ve teknik varlıklarda (container) işleniş biçimleri kapsamında kuruluşların sahip olduğu bilgi varlıklarına ve olası tehditlerin, güvenlik açıklarının nasıl oluşabileceğine odaklanmaktadır.

OCTAVE Allegro'nun geliştirilmesinde süreç adımlarının en aza indirilmesine önem verilmektedir. Allegro yönteminde kullanım kolaylığı sağlanarak minimum kaynak gereksinimiyle anlamlı sonuçların elde edilmesi desteklenmekte, değerlendirme sürecinin uzun vadeli tekrarlanabilirliği sağlanmaktadır. Workshop tabanlı veri toplama süreçleri basitleştirilerek çalışma sayfaları (çalıştay) ve yapılandırılmış rehberlik ile değiştirilen OCTAVE Allegro yönteminde, analiz ekibi dışında sürece kaynak eklenmesi azaltılmakta, çalışma sayfalarının programlanması ve koordine edilmesiyle ilgili genel giderler ortadan kaldırılmaktadır. Mevcut OCTAVE yöntemlerinde varlıklar, insanlardan bilgiye, sistemlere, hizmetlere, uygulamalara, donanıma ve yazılıma kadar uzanan alanı kapsamaktadır. Bu varlık türlerinin tümü risk değerlendirmesi için önemli olsa da bazı kullanıcılar bilgi dışındaki varlıklarla başlamayı kafa karıştırıcı bulmaktadır; çünkü bazen risk değerlendirmesi için çok geniş veya çok dar olan varlık tanımlarına yol açmaktadır. OCTAVE Allegro yönteminin birincil odak noktası bilgi varlığıdır. Kuruluş için önemli olan diğer tüm varlıklar, bağlı oldukları bilgi varlıkları bağlamında belirlenir ve değerlendirilir. Bu, kapsamla ilgili olası karışıklığı ortadan kaldırır ve daha sonra yetersiz tanımlanan, değerlendirme kapsamı dışında olan veya daha fazla ayrıştırılması gereken varlıklar için kapsamlı veri toplama ve analiz yapılması olasılığını azaltır. Bu yöntem, iç kontrol sistemini modernleştirmek ve bir işletmenin kontrol hedeflerine ulaşmasını sağlamak için kullanılabilir.

OCTAVE Allegro metodolojisi dört aşamaya bölünmüş sekiz adımda gerçekleştirilmektedir. Bunlar; katılımcılar tarafından yürütülen faaliyet alanları, kurumsal yönergelere uygun olarak risk ölçümü için değerlendirme kriterleri

geliştirmesi, kuruluşun misyonu, kurumsal hedefleri ve kritik başarı faktörleri vb., kuruluş için net sınırları oluşturmak, güvenlik gereksinimlerini belirlemek ve tüm kapsayıcılarını tanımlamak için herhangi bir kritik bilgi varlığının profilinin hazırlanması; kuruluş/departman bağlamında varlıklara yönelik yapılandırılmış bir süreç aracılığıyla tanımlanan ve belgelenen tehditlerin belirlenmesi, tehdit bilgilerine dayalı olarak risklerin tanımlandığı ve analiz edildiği ve bu riskleri ele almak için azaltma stratejilerinin geliştirildiği risklerin belirlenmesi ve azaltılması şeklinde sıralanmaktadır. Süreçteki her adımdan elde edilen çıktılar, daha sonra süreçteki bir sonraki adımda girdi olarak ele alınmaktadır. OCTAVE Allegro yöntemlerinin sekiz adım ve faaliyet alanları arasındaki ilişki Şekil 1'de gösterilmektedir.



Şekil 1. *OCTAVE ALLEGRO Yöntemi*

OCTAVE Allegro yöntemlerinin sekiz adımı aşağıda kısaca açıklamıştır.

1. Risk Ölçüm Kriterlerinin Oluşturulması: OCTAVE Allegro sürecindeki ilk adım, kuruluşun misyon ve iş hedefleri üzerindeki risk etkilerini değerlendirmesi için kullanılacak sürücüleri belirlemektir. İlk adımın bir parçası olan sürücüler, gerçekleşen bir riskin etkilerinin değerlendirilebileceği ve bir değerlendirmenin temelini oluşturan nitel ölçüler olan risk ölçüm kriterine yansıtılmaktadır. Doğru bir değerlendirme ile elde edilen risk ölçüm kriterleri, riskin nasıl azaltılacağına ilişkin kararların birden fazla bilgi varlığı ve işletme/departman birimi için tutarlı olmasını sağlamaktadır. Kuruluşlar için belirli alanlardaki bir etkinin kapsamını değerlendirmenin yanı sıra hangi etki alanlarının en önemli olduğunun bilinmesi de önemli olmaktadır. Bazı kuruluşlarda müşteri tabanıyla olan ilişkisi üzerindeki etki, yönetmeliğe uygunluğundaki etkiden daha önemli olabilmektedir. OCTAVE Allegro yönteminde, etki alanlarının önceliklendirilme işlemi de ilk adımda gerçekleştirilmektedir.

2. Bilgi Varlığı Profilinin Geliştirilmesi: OCTAVE Allegro metodolojisi, kuruluşun bilgi varlıklarına odaklanmakta ve Adım 2, bilgi varlıklarının benzersiz özelliklerinin, kalitesinin, özelliğinin ve değerinin tanımlandığı profil oluşturma sürecini başlatmaktadır. Metodolojinin profil oluşturma süreci, varlığın açık ve tutarlı bir şekilde tanımlanmasını, sınırlarının belirli olarak çizilmesini ve varlık için güvenlik gereksinimlerinin yeterince tanımlanmasını sağlamaktadır. Her bir varlığın profili, sonraki adımlarda tehdit ve risklerin tanımlanması için temel oluşturan tek bir çalışma sayfasında tutulmaktadır.

3. Bilgi Varlığı Container'larının Tanımlanması: *Container*, ana işlemcilere paralel ancak izole olarak bilgi varlıklarının depolandığı, taşındığı ve işlendiği yerleri tanımlamaktadır. Bilgi varlıkları yalnızca bir kuruluşun sınırları içindeki *Container*'ların yanı sıra kuruluşun doğrudan kontrolünde olmayan *Container*'larda da bulunmaktadır. Bilgi varlığının içinde bulunduğu *Container*'lara yönelik herhangi bir risk, bilgi varlığı tarafından devralınmaktadır. Örneğin, birçok kuruluş BİT altyapısının tamamını olmasa da bir kısmını hizmet sağlayıcılara dış kaynak olarak sağlamaktadır. Bu hizmet sağlayıcıları, kuruluşun bilgi varlıklarını içeren *Container'*ları yönetmektedir. Bir hizmet sağlayıcı, yönettiği depolarda saklanan, taşınan veya işlenen bir bilgi varlığının güvenlik gereksinimlerinin farkında değilse, bilgi varlıklarını korumak için gerekli olan kontroller yeterli olmayabilir ve dolayısıyla varlıkları riske maruz bırakabilmektedir. Bu nedenle, bir bilgi varlığına ilişkin yeterli bir risk profili elde etmek için kuruluş, bilgi varlıklarının depolandığı, taşındığı veya işlendiği tüm konumları, kuruluşun doğrudan kontrolü dahilinde olsun veya olmasın tanımlamalıdır. OCTAVE Allegro yönteminin 3. Adımında analiz ekibi bir varlığın içinde veya dışında depolandığı, taşındığı ve işlendiği tüm *Container'ları* tanımlamakta ve bir bilgi varlığını içinde barındıran tüm depolarla eşleyerek risk için incelenmesi gereken sınırları ve koşulları oluşturmaktadır.

***4. Endişe Alanlarının Belirlenmesi*:** Bu adım, kuruluşun bilgi varlığını tehdit edebilecek olası koşullar veya durumlar hakkında beyin fırtınası yaparak risk tanımlama sürecini kapsamaktadır. Bu gerçek dünya senaryoları, endişe duyulan alanlar olarak adlandırılmakta, tehditleri ve bunlara karşılık gelen istenmeyen sonuçları temsil etmektedir. Endişe alanları, bir kuruluşa ve çalışma koşullarına özgü bir tehdidi karakterize etmektedir. Bu adım,

bir bilgi varlığı için tüm olası tehdit senaryolarının tam listesini çıkarmak yerine analiz ekibinin aklına gelen durumları veya koşulları hızlı bir şekilde yakalamayı amaçlamaktadır.

5. Tehdit Senaryolarının Tanımlanması: Adım 5'in ilk yarısında, önceki adımda yakalanan endişe alanları, tehdide ait özellikleri detaylandıran tehdit senaryolarına genişletilmekte ancak bu endişe alanlarından geliştirilen tehditlerin toplanması, kuruluşun bilgi varlığına yönelik olası tehditlerin etkin bir biçimde değerlendirilmesini sağlamamaktadır. Bu nedenle, Adım 5'in ikinci yarısında, tehdit senaryoları incelenerek çeşitli ek tehditler göz önünde bulundurulmaktadır. Tehdit senaryolarına ait genellikle tehdit ağacı olarak adlandırılan yapı Tablo 1.'de verilmiştir.

TEHDİT AĞACI	TANIMLAR
Teknik Araçları Kullanan Kişiler	Kuruluşun teknik altyapısı aracılığıyla veya bir bilgi varlığını barındıran *container'a* (teknik varlık) doğrudan erişim yoluyla oluşan tehditleri temsil etmektedir. Kişi(ler) tarafından doğrudan eylem gerektirmekte, kasıtlı veya tesadüfi olabilmektedir.
Fiziksel Erişime Sahip Aktörler	Bilgi varlığına veya bilgi varlığını barındıran *container'a* fiziksel erişimden kaynaklanan tehditleri temsil etmektedir. Kişi(ler) tarafından doğrudan eylem gerektirmekte, kasıtlı veya tesadüfi olabilmektedir.
Teknik Problemler	Kuruluşun bilgi teknolojisi ve sistemleriyle ilgili sorunlardır. Örneğin; donanım kusurları, yazılım kusurları, kötü niyetli kod (ör. virüsler) ve sistemle ilgili diğer sorunlar yer almaktadır.
Diğer Problemler	Kuruluşun kontrolü dışında olan sorunlar veya durumlardır. Bu tehdit kategorisi, doğal afetleri (örneğin, sel, deprem) ve kritik altyapıların (örneğin, güç kaynağı) kullanılamaması gibi karşılıklı bağımlılık risklerini içermektedir.

Tablo 1. *OCTAVE Yönteminden Geliştirilen Tehditler*

İlgili alanlardan türetilen tehdit senaryoları, bu tehdit ağaçlarından bir veya daha fazlasına karşılık gelebilir. Bilgi varlıklarına ait tehditlerin sağlıklı bir şekilde değerlendirilmesi için, tehdit ağacının her bir dalının dikkate alınması önemli olduğundan birden fazla tehdit senaryosu anketi geliştirilmektedir. Bu adım aynı zamanda tehdit senaryolarının açıklamasında olasılığın değerlendirilmesi için bir fırsat sağlayarak senaryolardan hangisinin daha olası olduğunun belirlemesine yardımcı olmaktadır. Bununla birlikte, özellikle güvenlik açıkları ve olaylarla ilgili olarak olasılığı doğru bir şekilde ölçmek zor olduğundan, olasılık OCTAVE Allegro metodolojisinde niteliksel olarak yüksek, orta veya düşük olarak ifade edilmektedir.

6. Risklerin Belirlenmesi: Adım 5'te belirlenen tehditler aracılığıyla Adım 6'da herhangi bir tehdidin gerçekleşmesi durumunda kuruluş için olası sonuçlar yakalanarak risk denklemi tamamlanmaktadır. Bir tehdidin kuruluş üzerinde birden fazla potansiyel etkisi olabileceğinden bu adımda yer alan faaliyetler, riskin çeşitli sonuçlarının yakalanmasını sağlamaktadır.

7. Risklerin Analiz Edilmesi: Değerlendirmenin 7. Adımı olan risklerin analiziyle, kuruluşun tehditten ne ölçüde etkilendiğine ilişkin basit bir nicel ölçüm hesaplanmaktadır. Bu göreceli risk puanı, çeşitli etki alanlarının göreceli önemine ve olası bir riskin sonucunun kuruluşu ne ölçüde etkilediğini göz önünde bulundurarak türetilmektedir.

8. Risk Azaltma Yaklaşımının Seçilmesi: OCTAVE Allegro sürecinin son adımında ise kuruluşlar belirledikleri risklerden hangilerinin azaltılması gerektiğini belirleyerek bu riskler için risk azaltma stratejisi geliştirmektedir. Risklerin, göreceli risk puanlarına göre önceliklendirilmesinin ardından varlığın değerini ve güvenlik gereksinimlerini, içinde bulunduğu *container*'ları ve kuruluşun çalışma ortamını dikkate alan risk azaltma stratejileri geliştirilmektedir.

4 Sonuç

Kullanılan güvenlik önlemlerinden etkilenen ve en önemli amacı kuruluş içinde bilgi işlem güvenliğinin sağlanması olan tüm bilgi sistemi bileşenleri, kuruluşun güvenlik sistemini oluşturmaktadır. Güvenlik önlemleri yeni bilgi sistemi bileşenleri oluşturabilmekte ve yeni önlemleri gerekli kılabilmektedir. Bu nedenle tedbirler tek seferlik, dönemsel veya kalıcı uygulama için planlanabilmektedir. Bilgi sistemleri güvenliğinde, bir tehlikeyi önleyici tedbirler, tespit edici tedbirler ve düzeltici tedbirler birbirinden ayrılmalıdır. Bu nedenle, OCTAVE, bilgi güvenliği alanında risk değerlendirmelerini yürütmek için fiili bir standart olarak kabul edilmektedir. Güvenlik ve iş sürekliliği esnekliğe dönüştükçe ve kuruluşlar operasyonel riski yönetmenin bir yolunu aradıkça, ilgili topluluk büyümeye devam etmektedir. Yöntemin pratikte uygulanabilirliği ve daha büyük işletmelerde kullanılması için çeşitli yollar geliştirilmeye devam edilmektedir. Genel risk portföyünün bir parçası olarak operasyonel riski etkin bir şekilde yönetmenin ve aynı zamanda altta yatan süreçleri sürekli iyileştirmenin önemi OCTAVE yöntemlerinin odak noktasını oluşturmaktadır.

Bilgi teknolojisi ile risk yönetiminin; finansal etki, güvensiz sistemler nedeniyle azalan itibar, ticari faaliyetlerin durdurulması, değerlendirilebilir varlıkların (sistem ve veriler) başarısızlığı ve gecikmiş karar verme sürecini içerebilecek zararların etkisini azaltması beklenmektedir. OCTAVE Allegro, bilgi varlıklarına ve bu bilgileri destekleyen verilere odaklanmaktadır. Kurumsal iş hedeflerine ulaşmak için gereken güvenlik düzeyine ilişkin

bilgi, uzmanlık, yetenek, iç kontrol ve anlayışı sürdürmek için bilgi teknolojisi çalışanlarına işletmenin bilgi sistemleri hakkında eğitim vermek önemlidir (Sardjono and Cholik, 2018). OCTAVE Allegro değerlendirmesinin tek bir bilgi varlığı üzerinde kullanılması amaçlandığından birden fazla bilgi varlığını değerlendirmek isteyen kuruluşların, risk değerlendirme kapsamına dahil olan her bilgi varlığı için süreci (Adım 2, Faaliyet 3'ten başlayarak) tekrarlaması gerekmektedir.

Kaynakça

- Ak, M.F., Gül,M., (2019), AHP–TOPSIS integration extended with Pythagorean fuzzy sets for information security risk analysis, Complex & Intelligent Systems,5, 113-126.
- Aleuatdinovich, B.G., Usarovna, Y.S., (2022), Information Security in the Financial and Banking System of the Republic of Uzbekistan, Central Asian Journal Of Mathematical Theory And Computer Sciences, 3 (2), 1-4.
- Chen,J., Zhu, Q., (2019), Interdependent Strategic Security Risk Management with Bounded Rationality in the Internet of Things, Information Forensics and Security,1-13.
- Dhillon, G. and Backhouse, J., (2000), *Information System Security Management in the New Millennium*, Communications Of The Acm, 43 (7), 125-128.
- Dubois, E., Heymans, P., Mayer, N. and Matulevi˘cius, R., (2010), *A Systematic Approach to Define the Domain of Information System Security Risk Management*, Intentional Perspectives on Information Systems Engineering, 289–306.
- Jouini, M., Arfa Rabai, L., Aissa,A., (2014), *Classification of security threats in information systems,* 5th International Conference on Ambient Systems, Networks and Technologies, Procedia Computer Science 32,489 – 496.
- Koduah-Tweneboah, S. and Buchanan, W. J., (2018), *Security Risk Assessment of Critical Infrastructure Systems: A Comparative Study*, Sectıon A: Computer Science Theory, Methods And Tools The Computer Journal, 1-18.
- Kokkonda, J., (2022), IoT Dialectical and Security Threats: A cybernated inquisition schema for IoT systems, JAC: A Journal Of Composition Theory,15 (3),14-20.
- Kuhlen, R., Semar, W., (2013), *Sicherheit von Informationssystemen*, Grundlagen der praktischen Information und Dokumentation, Dietmar Strauch (Hrsg.), 6. Ausgabe. Walter de Gruyt, Berlin, 466-478.
- Kuzminykh, I., Ghita, B., Sokolov, V. and Bakhsh, T., (2021), *Information Security Risk Assessment*, Encyclopedia 2021, 1, 602–61.
- Leonard,A., Anggito, N., Sialagan,F., Suroso, J.S., (2020), nformation System Security Risk Management E-Learning Using FMEA in University, International Journal of Advanced Trends in Computer Science and Engineering, 9(5), 7565-7568.
- Li, X., Al-Shawabkeh, M. and Li, Z., (2018), *Security Risk Management Approach for Improving Information Security Return of Investment*, Recent Developments in Data Science and Business Analytics Proceedings of the International Conference on Data Science and Business Analytics, Madjid Tavana and Srikanta Patnaik (Eds.), Springer International Publishing AG, 209-216.
- Li, X., Li, H., (2018), *A Visual Analysis of Research on Information Security Risk by Using Cite Space*, IEEE Access,6, 63243- 63257.
- Matulevi˘cius, R. and Savukynas,R., (2019), *Application of the Reference Model for Security Risk Management in the Internet of Things Systems*, Databases and Information Systems X, A. Lupeikiene et al. (Eds.), The authors and IOS Press,65-78.
- Prieß, A., Hoppe, G., (2004), *Modellierung der Sicherheit von Informationssystemen mit DROPS*, Diskussionsbeitrag, No. 301, Universität Hannover, Wirtschaftswissenschaftliche Fakultät, Hannover,1-18. https://www.econstor.eu/bitstream/10419/22413/1/dp-301.pdf
- Rahmani, K.R., Rana, S. and Hossan,A., (2022), Lightweight Cyber Security for Decision Support in Information Security Risk Assessment, EJECE, European Journal of Electrical Engineering and Computer Science, 6 (1),24-31.
- Sardjono, W. and Cholik, M. I., (2018), Information Systems Risk Analysis Using Octave Allegro Method Based At Deutsche Bank. 2018 International Conference On Information Management And Technology (Icımtech). Doi:10.1109/İcimtech.2018.8528108
- Sukri, M. and Riadi, I., (2021), Risk Management Analysison Administration System Using Octave Allegro Framework. *International Journal Of Computer Applications*, *975*, 8887.
- Suroso, J. S. and Fakhrozi, M. A., (2018), Assessment of information system risk management with octave allegro at education institution. *Procedia Computer Science*, *135*, 202-213.

- Szczepaniuk, E.K., Szczepaniuk, H., Rokicki, T., Klepacki,B., (2020), *Information security assessment in public administration*, Computers & Security, 90, 1-27.
- Wang, Y., (2021), *Research on Security of Accounting Information System in the Era of Big Data*, Journal of Physics: Conference Series,1-7.
- Wei, R. and Yao, S., (2021), *Enterprise Financial Risk Identification and Information Security Management and Control in Big Data Environment*, Hindawi-Mobile Information Systems, 1-6.
- Zekıć, B. H. and Mılıć, D. C., (2016), ICT Security Risk Assessment in Higher Education Institutions. *Under The Auspices Of The President Of The Republic Of Croatia*, 138.