GÜVENLİK ÇÖZÜMLERİ METODOLOJİSİ

Securitas

GÜVENLİK ÇÖZÜMLERİ METODOLOJİSİ

HAZIRLAYAN
Feramuz ÇALIŞKAN

KATKIDA BULUNANLAR
Hüseyin ERİM
Berti BORA
Gökhan USTA
Aygen ÜNDAN
Memet HANLIOĞLU
Emre ERDAL
Adem YÜKSEL
Alp KARABAŞ
Volkan AKSU
Can ULUATAM

YAYINA HAZIRLAYAN
Elif Duygu KOCA

REDAKSİYON
İrem YEŞİL

TASARIM
Dwt Mandalina

BASKI
Emsal Matbaa Tanıtım

GÜVENLİK ÇÖZÜMLERİ METODOLOJİSİ

Securitas

Securitas

Önsöz

Hayatımızın her alanında en temel gerekliliklerin başında gelen güvenliğimizi en uygun maliyetler ile sağlamak ve bunu sürdürülebilir kılmak çözülmesi zor bir denklem.

İşte bu zor denklemi metodolojik bir yöntem ile çözebilmek için yıllar boyunca Securitas Türkiye bünyesinde birikmiş deneyim üzerinde 2015 yılından bu yana düşündük, çalıştık, çizdik, bozduk, yazdık, düzelttik, sınadık, yine düzelttik ve bu kitapta bulacağınız metodolojiyi geliştirdik.

Bu kitap bizim yaşayan bir kitabımız. Kendini edindiği tecrübeler ile geliştirecek, yeni yeni bilgi ve teknikleri içine katacak. Türkiye'de özel güvenlik sektörüne yön veren bir marka olarak bugün yaptığımız işin inceliklerini sizlerle paylaşıyor olmak mutluluk verici.

Bu metodolojiye yaslanarak güvenliğinden sorumlu olduğunuz tesislerin en akıllı şekilde korunabileceğini söyleyebiliriz.

Güvenlik Sektöründe Bilgi, İnsan ve Teknolojinin entegrasyonunun en rafine karşılığı olan Securitas Güvenlik Metodolojisi ile liderlik ederken ayak izlerimizin yol göstermesi dileğiyle ve

Hevesle benimseyeceğiniz umuduyla;

Saygılarımla,
Murat Kösereisoğlu
Securitas Türkiye Ülke Başkanı

GİRİŞ

Her iş için olduğu gibi Güvenlik Dünyasında da; bir güvenlik hizmetinin daha önce sektörde yaşanan tecrübe ve bilimsel metotlarla yapılandırılması oldukça önemli. Ancak bu yolla işletme risklerini doğru tespit edebilen, risklerin etkisini en aza indirebilmek için en uygun çözümü geliştiren ve yakaladığı kalite standartlarını sürdürebilen bir güvenlik hizmeti tesis edilebilir.

Securitas Güvenlik Metodolojisi; bir güvenlik hizmetinin en başından sonuna kadar nasıl yapılandırılacağı, risklerin nasıl tespit edilip ölçeklendirilebileceği, kurumların risk yönetim sürecine etki eden önemli kavramların neler olduğu, en uygun çözümün hangi hiyerarşi ile geliştirilebileceği ve kalite standartlarını yükseltmeye ve sürdürmeye katkı sağlayacak uygulamaların neler olabileceğine ilişkin önemli açıklamalarda bulunuyor. Bu çalışmadan, görevi her ne olursa olsun Güvenlik Sektöründe faaliyet gösteren, Güvenlik Hizmeti satın alan veya Üniversitelerde ilgili bölümlerde akademik faaliyetlerini yürüten herkes faydalanabilir. Şüphesiz bu çalışmanın birçok gelişim alanı tespit edilecektir, böylesine dinamik bir alanda bu kaçınılmazdır da. Bu nedenle bu metodolojinin bu güne kadar olduğu gibi bu günden sonra da sürekli kendini geliştiren, dönüştüren ve yenilenen bir çalışma olması hedefleniyor.

Bu Metodolojisi, Securitas Türkiye çalışanlarının toplam tecrübelerinin bir çıktısı niteliğinde. Securitas Türkiye'de görev yapan alanlarında uzman bir çok değerli isim bu çalışmaya çok önemli katkılarda bulundu. Uzun yıllara dayanan tecrübe ve yine Güvenlik Dünyasına ilişkin en güncel teknolojik gelişmelerle harmanlanan Securitas Güvenlik Metodolojisinin, Güvenlik Sektörüne katkı sağlamasını umuyoruz.

Feramuz Çalışkan

Güvenlik Süreçleri ve Kalite Müdürü

“Yüksek verimlilik ve sürdürülebilirlik için güvenlik hizmetinin, hizmet öncesi ve hizmet sürecini de kapsayacak bir yöntem ile standart bir “sistem” haline getirilmesine ihtiyaç vardır.”

Güvenlik Hizmeti ve Metodolojik Yaklaşım

Organizasyonlar, güçlükleri gittikçe artan ve karmaşıklaşan bir ortamda faaliyetlerini sürdürmektedirler. Belirsizliği giderek artan bu çevre içinde organizasyonlara ilişkin kurumsal beklentiler de artmaktadır. Artan beklentiler ve karşı kaşıya bulunan belirsizlik, kurumları faaliyetlerinin sonucunu önemli ölçüde etkileyebilecek risklerle karşı karşıya bırakmaktadır.[1] Bu pazar koşulları içerisinde; Securitas tarafından üretilen önleyici güvenlik mahiyetindeki güvenlik hizmeti ile bu hizmeti alan kurumun risklerinin optimum çözümlerle en aza indirilmesi ya da tamamen ortadan kaldırılması hedeflenir. Verilen güvenlik hizmetinden etkilenen birden fazla taraf vardır.

"Pazar koşulları zorlaşıp riskler çeşitlenirken kurumlara ilişkin beklenti artıyor."

Örneğin, hizmet veren güvenlik şirketi ile hizmet alan ana taraflar iken; kamu otoritesi, hizmet veren ile hizmet alanın çeşitli konulara ilişkin tedarikçileri, tesis çalışanları, komşu tesisler gibi taraflar bu süreçten etkilenen diğer taraflardır. Yine güvenlik hizmeti sürecini etkileyen birden fazla alan vardır. Yasal zorunluluklar, risk etkisi, teknolojik gelişmeler, ihtiyaçlar, lokasyon, iş kolu güvenlik hizmeti sürecine etki eden bazı önemli faktörlerdir. Görüldüğü gibi, birden fazla tarafı ve dikkat edilmesi gereken aşamaları olan güvenlik hizmetinin; bir sistem ya da başka bir deyişle bir metot ile yapılandırılması son

[1] *Hopkin, 2017*

derece önemlidir. O halde, güvenlik hizmetinin, hizmet öncesi ve hizmet sürecini de kapsayacak bir yöntem ile standart bir "sistem" haline getirilmesine ihtiyaç vardır. Bu durum, güvenlik hizmetinin bir yöntem ya da başka bir deyişle bir metodoloji ile başlatılmasını, sürdürülmesini ve kontrol edilmesini gerekli kılar.

Bu durumda;
— İzlenecek yöntemin,
— Bu yöntemin geliştirilecek çözümlere nasıl yansıyacağının,
— Çözümlerin nasıl uygulanacağının ve
— Uygulamaya ilişkin kontrollerin nasıl sağlanacağının bilinmesi gerekir.

Bu gereklilik bir güvenlik şirketi için tüm bu süreçlere ilişkin bir metodolojiye sahip olmayı zorunlu kılar.

Peki, daha geniş anlamıyla metodoloji ya da metodolojik yaklaşım nedir?

“Metodolojik yaklaşım kurumların zorlu yolculuğunda onlara kılavuzluk eden bir yol haritasıdır.”

Metodolojik Yaklaşım Nedir?

Metodoloji kurumların hedefleri için ilerledikleri yolda bir "yol haritasıdır."

Metodoloji[2], ilk akla gelen haliyle; "kurumların faaliyetlerini etkin olarak gerçekleştirmeleri ve çok yönlü hedeflerine ulaşabilmeleri için uyguladıkları genel program veya takip edilmesi gereken yol haritasıdır" şeklinde tarif edilebilir.

İşletme ve/veya organizasyonların uyguladıkları metodoloji, kurumların mevcut ve gelecekteki işlevlerini ortaya koymaktadır. Yani hedeflere ulaşmak için bir yol haritası olarak kullanılan metodoloji, amaçları tanımlayan ve amaçlara ulaşmaya yardımcı olan tüm yöntemleri ifade etmektedir. Kurumun iç dinamikleri ve yetenekleriyle, dış çevrenin işlevlerini koordine edecek faaliyetlerin belirlenmesinde etkin rol oynamaktadır.

Güvenlik dünyasında metodolojinin anlamı nedir?

Güvenlik uygulamaları kapsamında "metodoloji"; güvenlik kurgusunun en doğru şekilde yapılandırılabilmesi için gerekli bakış açısını sunan bilgileri, teknikleri, yaklaşımları ve analiz yöntemlerini kapsayan bilimsel yaklaşımdır.

Metodolojide esas olan; bir konu hakkında toplanan bilgilerin bir düşünce gelişimine, düşüncenin sınıflandırılmasına ve analiz edilmesine katkı sunabilmesidir. Ulaşılan sonuçlar tüm paydaşlarda güven duygusunu beslerken güvenlik hizmetinin

[2] Metodoloji: Güvenlik uygulamaları kapsamında "metodoloji"; güvenlik kurgusunun en doğru şekilde yapılandırılabilmesi için gerekli bakış açısını sunan bilgi, teknikler, yaklaşımlar ve analiz yöntemlerini kapsayan bilimsel yaklaşımdır.

de verimlilik prensibi ile yapılandırılmasını sağlamalıdır. Bu gereklilik, sonuçları ve etkileri gözlemlenmiş bir dizi faaliyet ya da yaklaşım arasından en verimlisinin yöntem olarak benimsendiği bilimsel yaklaşımı zorunlu kılar. Metodoloji, bu bilimsel yaklaşımın süreç olarak adımlarının ortaya koyulması ve ulaşılan sonuçların başkaları tarafından, farklı zamanlarda tekrarlanabilir olmasıdır. Örnek olarak; metodolojinin tekrarlanabilir olması özelliği sayesinde benzer risk ve özellikleri olan birbirinden uzak bir çok yerleşkede bakış açısı, kullanılan yöntemler, oluşturulan kurallar ve benzer ihtiyaçlar için üretilen çözümler açısından benzer sonuçlar üretebilme imkânı sağlar ve güvenlik hizmeti standart hale getirebilir. Bu özellik, güvenlik hizmetinin **standart** hale getirilmesi ve **sürdürülebilir** verimliliğin sağlanması açısından son derece önemlidir.

Metodolojinin tekrarlanabilir olması farklı lokasyon ve farklı segmentlerde yürütülen güvenlik hizmetinin standart hale getirilmesini sağlar.

“Artan rekabet koşulları, değişen pazar yapısı, karmaşık ve çok katmanlı hale gelen güvenlik riskleri; güvenlik hizmetinin metodolojik bir yaklaşımla yapılandırılmasını zorunlu kılar.”

Metodolojiye Neden İhtiyaç Var?

Günümüz güvenlik sorunlarının giderek çok boyutlu ve karmaşık bir hal almış olması sebebiyle çözüm yolları da birden fazla katman içeren, birden fazla birim / departmanın koordinasyonunu zorunlu kılan bir noktaya gelmiştir. Bu çerçevede, güvenlik uygulamalarının metodolojik bir yaklaşımla değerlendirilmesi kaçınılmazdır. Bir güvenlik şirketi metodolojik bir yaklaşıma ya da başka bir deyişle "Güvenlik Metodolojisine" ihtiyaç duyar, çünkü Metodolojik Yaklaşım;

— Karar alma sürecinin haritalanmasıdır. Bu yönüyle, hizmet üretme sürecinin tüm paydaşları için yol gösterici bir kılavuz niteliğindedir.
— Organizasyon dışı faktörlerin dikkate alınmasıyla karar alma sürecinin işletilmesine katkı sağlar, böylelikle karar sürecinin en doğru zemine oturmasına yardımcı olur.
— Planları ya da faaliyetleri olumsuz yönde etkileyebilecek tüm faktörlerin sistematik şekilde tespit edilebilmesine ve bu engellerin ortadan kaldırılmasına katkı sağlar.
— Kurum amaçlarına ulaşmayı kolaylaştıran bir yol haritası, bir kılavuz niteliğindedir. Bu nedenle Metodolojinin belirlenmesi için kurum amaçları ve bu amaçlara ulaşmak için kullanılacak kurum stratejisinin belirlenmesi gerekir.
— İş faaliyetlerinin ve sürekliliğinin planlanmasını sağlar.
— Güvenlik hizmetinin yapılandırılması, başlatılması, uygulanması ve kontrol edilmesi sürecinde, ilgili tüm paydaşlar arasında koordinasyonu sağlar.

Güvenlik sorunları çok katmanlı ve karmaşık hale geldi, bu pazar koşullarında güvenlik uygulamalarının metodolojik bir yaklaşımla yapılandırılması gerekir!

— Uygulamaların yasal mevzuat, ulusal ve uluslararası kalite standartları ve sektörel gereklilikler çerçevesinde kontrol edilmesine yardımcı olur.
— İşletmelerin faaliyetlerini doğru olarak hazırlamaları için yol gösterici niteliktedir.

Dolayısıyla kurumların kimliğinin oluşması ve yaşatılması sürecinde, vizyon ve misyonunun belirlenmesi için gerekli hedeflerin oluşturulmasına katkı sağlar.

Güvenlik metodolojine sahip bir güvenlik şirketi riskleri önlemek veya risklerin etkisini azaltmak açısından etkin bir işleve sahiptir. Ayrıca doğru belirlenen ve tüm yönleriyle başarıyla uygulanan bir metodoloji, çok önemli bir rekabet avantajı sağlar.

Bir güvenlik şirketi için farklı tesis, kurum veya işletmelerde hatta farklı şehirlerde yerine getirilen güvenlik hizmeti; öncelikle bağlı olunan kanunlar, sektör standartları ve Kurumların beklentileri nedeniyle sistematik bir yaklaşımı zorunlu kılar. Bütün iş kolları için olduğu gibi güvenlik sektörü çalışanları için de işlerine dair derinlemesine bilgi sahibi olmak, yeni çözüm ve fikir geliştirebilmek büyük öneme sahiptir. Derinlemesine bilgi sahibi olmak ve yenilikçi fikirler geliştirebilmek için daha

önce geliştirilmiş fikir ve çözümlerin bilinmesi, bu bilgi eşliğinde sistematik bir yaklaşımla güncel detayların incelenmesi gerekir. Ancak bu yolla güvenlik uygulamalarına dair detayları bir bütünlük içerisinde ele alma imkânı ortaya çıkar. Güvenlik uygulamalarına ilişkin sorumluluklar diğer paydaşların da etki ve katkıları hesaba katılarak "metodolojik" bir yaklaşımla ele alındığında;

— Kanun ve kalite standartlarına uygun,
— Kurumların beklentisine cevap veren ve Kurumların ihtiyaç ve beklentilerini en doğru şekilde ortaya koymayı sağlayan,
— Verimli,
— Etkili,
— Sürdürülebilir,
— Rekabet avantajı yaratan bir sonuca ulaşmak mümkün olacaktır.

Bir tesisi ve tesisin tüm ihtiyaçlarını derinlemesine anlamak ve yenilikçi fikirler ortaya koyabilmek için geçmişten gelen bilgi eşliğinde sistematik bir yaklaşımla detayların incelenmesi gerekir.

Metodolojik yaklaşımda esas olan bir konu hakkında toplanan bilgilerin bir düşünce gelişimine, sınıflandırılmasına ve analiz edilmesine katkı sunabilmesidir. Tam bu noktada "Güvenlik Metodolojisi", üretilen güvenlik hizmetine dair izlenmesi gereken adımları tarifleyen bir yol haritası olarak ilgili taraflara kılavuzluk eder.

Securitas Güvenlik Metodolojisi (SGM), Kurumun güvenlik ihtiyaçlarını karşılayan optimum **güvenlik çözümlerinin üretilebilmesi ve sürdürülebilmesi** amacıyla izlenmesi gereken adımları açıklar. Ayrıca bu bağlamda uygulayıcılar için yol gösterici kılavuz niteliğinde olan ve güvenlik süreçlerini kapsayan yapıdır.

Kurumlar ile uzun soluklu, karşılıklı fayda prensibine dayalı ilişkiler tesis edebilmesinde Securitas Güvenlik Metodolojisi ile ifade edilen süreçlerde yapılan işlemlerin büyük önemi vardır. Bundan dolayı Securitas bünyesinde görev yapan güvenlik profesyonellerinin, Securitas Güvenlik Metodolojisinde bahsi geçen hususlarla ilgili büyük bir hassasiyet ve titizlik göstermesi beklenir.

Tüm Securitas çalışanlarının sahip oldukları pozisyonlar çerçevesinde görev ve sorumlulukları bulunmaktadır. SGM, öncelikle bağlı olunan kanunlar, Securitas prosedür ve talimatları yanında; güvenlik uygulamalarının benzer standartlarda ve yüksek kalitede yürütülmesini sağlayan bir kılavuzdur.

Securitas'ın iş ortakları ile uzun soluklu, karşılıklı fayda sağlayan ilişkiler kurabilmesinde Securitas Güvenlik Metodolojisi büyük rol oynar.

“Güvenlik Metodolojisi ile iş sürekliliğini ve verimliliğini etkileyebilecek yüksek seviyedeki riskler ya tamamen ortadan kalkar ya da kabul edilebilir, yönetilebilir sınırlara indirilir.”

Securitas Güvenlik Metodolojisi

Securitas, zaman içinde kazandığı bilgi ve deneyimi sistematik bir tabana oturtarak Securitas Güvenlik Metodolojisini (SGM) oluşturmuştur.

Securitas'ta, güvenlik hizmetinin yapılandırılması ve sürdürülmesi sürecinde uygulanan hareket tarzları, zamanla sistematik bir tabana oturtulmuştur. Bu doğrultuda Securitas Güvenlik Metodolojisi (SGM), Securitas İş Yönetim Politikasına uygun olarak;

— Farklı segmentlerdeki Kurum ihtiyaçlarına cevap veren
— Etkinliği yüksek güvenlik çözümünün optimum maliyetlerle tasarlandığı, yüksek katma değerli,
— Bütünleşik bir güvenlik çözümü amaçlayan,
— İleri teknolojileri ve verimliliği ön plana alan entegre güvenlik çözümleri sunan,
— Hizmet noktalarının tamamında yüksek kalite standartlarını yakalayabilmek için Securitas Türkiye'nin ilgili tüm birimleri tarafından güvenlik süreçlerinin ortak bir anlayışla uygulanmasını sağlayan

yüksek riskleri kabul edilebilir / yönetilebilir sınırlara indirmeyi amaçlar.

Securitas'ın önceliği Kurumlara etkinliği yüksek maliyeti düşük güvenlik hizmeti vermektir. Güvenlik alanına dair sunduğu çözümlerle farklılaşma ve ayrışma özelliğine sahip olan Securitas'ın tüm faaliyetleri Kurum odaklı ve kaliteli hizmet verme stratejisi ile uyumludur. Securitas, bu strateji doğrultusunda Kurumlara daha etkin çözümler sunabilmek amacıyla faaliyet gösterdiği pazarı ortak yönlerine göre çeşitli kategorilere ayırır. Bu kategoriler segment ve hizmet yeri olarak gruplandırılır.

Örneğin "Endüstri" Securitas için bir segment iken Endüstri Segmenti altında "Fabrika" bir hizmet yeri "Depo" ayrı bir hizmet yeridir. Hizmet üretilen alanların segment ve hizmet yerleri olarak ayrıştırılması ortak ihtiyaçlar için ortak bazı uygulamaların yapılandırılmasına imkân verir. Securitas bünyesinde tüm segment

ve hizmet yerlerinde yürütülen güvenlik hizmeti SGM esasları çerçevesinde oluşturulurken, segment ve hizmet yerlerine özgü gereklilikler de yine bu esaslar çerçevesinde belirlenir.

Securitas Güvenlik Metodolojisi kapsamında hizmet yürütme prensiplerinin dikkatle uygulanması, esasları önceden belirlenmiş yöntemlerle kontrol edilmesi sürdürülebilirliğin sağlanmasına katkı sağlayacaktır.

Securitas Dünyanızın Daha Güvenli Hale Gelmesine Nasıl Yardımcı Oluyor?

Securitas sahip olduğu teknolojik kabiliyetler, dijital uygulamalar ve uzun yıllar içinde edindiği tecrübeyi; Securitas Güvenlik Metodolojisi ile Kurumların dünyasını daha güvenli hale getirmek için, Kurum ihtiyaçlarına uygun olarak kullanıyor.

Bu kapsamda Securitas Güvenlik Metodolojisi,

— Tesisin güvenlik risklerini tespit etmek, bu risklerin olasılık ve etkilerini göz önünde bulundurarak önceliklendirmek,
— Bu riskleri en etkin, düşük maliyetli ve sürdürülebilir çözümler ile kabul edilebilir sınırlara indirgemek ya da mümkün olduğu hallerde tamamen ortadan kaldırmak,
— Risklerin gerçekleşmesinin engellemek için **Caydırıcı** unsurların yapılandırılmasını sağlamak
— Risklerin gerçekleşme anını en uygun yöntemler ile **Algılamak ve Doğrulamak**,
— Riskin gerçekleşmesi halinde ilgili tehdit ve/veya risk unsurunu **Geciktirmek** ve hasarın büyümemesi için **Müdahale**nin en doğru ve etkin yöntemlerle yapılmasını temin etmek,
— Çözüm, iyileştirme ve geliştirme çalışmalarının yönetilmesiyle birlikte gerekli aksiyonların alınmasını sağlamak
— Süreçlerinin doğru bir şekilde uygulanıp uygulanmadığının denetlenmesini ve düzeltici/iyileştirici tedbirlerin alınmasını sağlamak amacıyla kullanılır.

Securitas Güvenlik Metodolojisi'nin Kapsamı

Securitas Güvenlik Metodolojisi'nin tüm adımlarının orta ve büyük ölçekli işletmelerde daha doğru ve daha kolay uygulama alanı bulacağı değerlendirilmektedir.

Securitas Güvenlik Metodolojisi'nden segment ve büyüklük gözetmeksizin tüm işletmeler güvenlik kurgusunu oluştururken ve yönetirken faydalanabilir. Ancak Securitas Güvenlik Metodolojisi'nin tüm adımlarının orta ve büyük ölçekli işletmelerde daha doğru ve daha kolay uygulama alanı bulacağı değerlendirilmektedir. Hedef uygulama alanında değişiklik olması halinde metodolojiden yaralanmakla birlikte metodolojinin adımlarında revize yapma ihtiyacı doğabilir.

“Securitas Güvenlik Metodolojisi verilerin toplanmasından gelişim alanlarının tespitine uzanan 5 adımda uygulanır.”

Securitas Güvenlik Metodolojisi'nin Adımları

Securitas Güvenlik Metodolojisi beş adımdan oluşmaktadır. Bu adımlar;

1. ***Mevcut Durum Analizi (MDA),***
2. ***Güvenlik Hizmeti Risk Değerlendirmesi (GRD),***
3. ***Çözümler,***
4. ***Uygulama,***
5. ***Kalite Kontroldür.***

Securitas Güvenlik Metodolojisi
Birinci Adım:

Mevcut Durum Analizi

Mevcut Durum Analizi

Mevcut Durum Analizi (MDA)'nin amacı, güvenlik hizmetine ihtiyaç duyan kurumu iyi tanımak ve kurumun o anki güvenlik durumunu net olarak ortaya koymak, anlık durumun fotoğrafını çekmektir.[3] **Mevcut Durum Analizi (MDA); güvenlik hizmeti sunulacak işletmenin genel özelliklerinin belirlenmesi, tanınması, mevcut güvenlik yapısının ve farkındalığının, idari ve operasyonel prosedürlerinin anlaşılmasıdır.** Bununla birlikte korunma ihtiyacı olan tesislerin, bölgelerin ve/veya yapıların içinde bulunduğu koşullar çerçevesinde, fiziksel olarak incelenmesi ve tespit edilen hususların gerçekte olduğu şekliyle raporlanmasıdır.

Metodoloji içerisindeki her bir adımda, bir önceki adımda elde edilen verilerden ve ulaşılan sonuçlardan yararlanılmaktadır. Bu kapsamda Mevcut Durum Analizi'nin doğru ve etkili bir şekilde yapılması bir sonraki aşamada gerçekleştirilecek **Güvenlik Hizmeti Risk Değerlendirmesi**'nin güvenilirliğini ve geçerliliğini etkileyecektir. Yetersiz bir gözlemle yapılan mevcut durum analizi sonucunda potansiyel riskler anlaşılamayıp değerlendirilemeyebilir ve bu durum ileride önemli güvenlik zafiyetlerinin oluşmasına sebep olabilir.

Mevcut Durum Analizi ile elde edilen verilerden tesisin risklerinin ve dolayısıyla güvenlik çözümlerinin oluşturulmasında istifade edilir.

---

[3]Mevcut Durum Analizi kurumun o andaki fotoğrafını çekmeyi yani mevcut durumu tespit etmeyi amaçlayan çalışmadır.

Mevcut Durum Analizinin tam ve doğru yapılması gelecekte ihtiyaç duyulacak çözümlerin doğru kurgulanmasına katkı sağlar. Çünkü, tesis ihtiyaçlarının ve ihtiyaçlara en uygun çözümlerin kurgulanması için, içinde yaşanılan koşulların tam ve doğru olarak ortaya koyulması gerekir.

Mevcut Durum Analizinin tam ve doğru yapılması gelecekte ihtiyaç duyulacak çözümlerin doğru kurgulanmasına katkı sağlar çünkü, tesis ihtiyaçlarının ve ihtiyaçlara en uygun çözümlerin kurgulanması için, içinde yaşanılan koşulların tam ve doğru olarak ortaya koyulması gerekir. Mevcut durumun doğru olarak ortaya koyulamaması ise gerek Securitas'tan hizmet alan Kurum, gerekse Securitas açısından istenmeyen sonuçlara neden olabilir. İlk adımın doğru atılması sonraki adımların tamamının doğru olması açısından kritik öneme sahiptir. Bu adımda Kurum ile koordineli bir şekilde çalışılır ve elde edilen veriler Kurumun bilgisine sunulur. Gerçekleştirilen MDA Kurum ile paylaşılarak doğru ve eksiksiz olduğu teyit edilmek amacı ile mutabakat sağlanır.

Mevcut Durum Analizinde aşağıdaki konular dikkate alınır.

1. MDA'nın yapılacağı tesise/binaya/bölgeye gidilmeden önce fikri genel bir fikir edinmek için ön hazırlık yapılır. Kurum ile ilgili internet sitesi vb. açık kaynaklardan erişilebilen bilgiler, Securitas bünyesindeki benzer birimlerde daha önceden meydana gelmiş olay ve hasarlar, tesisin bulunduğu bölgenin suç istatistikleri, benzer projelere ait talimatlar (talimatlar riskleri engellemek üzere hazırlandığından – olası riskler hakkında fikir verir), proje bölgesinin Google Earth görüntüleri vb. hususlar incelenir. Önden yapılan çalışma ile hem zaman kazanılmış olur hem de önceden faaliyetlerin nasıl yürütüleceğine ilişkin planlamalar daha etkili bir şekilde yapılır.

2. Kurum talepleri ile ilgili ilk bilgiler, Kurum temas bilgilerinin kaydedildiği Securitas sistemlerinden ve teması sürdüren Securitas çalışanlarından alınır.
3. MDA yapılmadan önce Kurumdan bir kılavuz personel sağlanması talep edilir ve çalışma kılavuz personel eşliğinde yapılır.
4. MDA yapılırken projenin segmenti belirlenir ve projede yer alan her bir hizmet noktası (örneğin; nizamiye (giriş kontrol noktası), çevre engelleri (ör. tel örgü veya duvarları), otoparklar, imalathaneler, ofis binaları vb.) incelenir.
5. İnceleme yapılacak yerlere sırasıyla gidilir. Her bir hizmet yerinde mevcut güvenlik tedbirleri, yürürlükte olan tedbirlere bağlı iyi uygulamalar ve varsa güvenlik zafiyetleri tespit edilir. Burada elde edilecek veriler sonraki adım olan risk analizi için temel oluşturmak üzere kullanılır.

Mevcut Durum Analizi binanın temeli gibidir. Temel ne kadar sağlamsa bina da o ölçüde sağlam olacaktır.

Mevcut Durum Analizi, Securitas Güvenlik Metodolojisi uygulamasının ilk adımıdır. Bu adımda tespit edilecek bilgiler ne kadar doğru olur, kurum ya da tesise ilişkin mevcut durum bilgisi ne kadar kesin ve net tespit edilirse sonraki adımların tamamı da bu doğru bilgi üzerine inşa edilebilir. Bu sebeple, Securitas Güvenlik Metodolojisi'nin Mevcut Durum Analizi adımı inşa edilen bir binanın temeli gibidir. Bir binanın temeli ne kadar doğru, detaylı düşünülmüş, sağlam ise bina da o denli güçlü olacaktır. Bu nedenle "temel" niteliğindeki Mevcut Durum Analizi mümkün olan en doğru ve detaylı şekilde yapılmalıdır. Ayrıca Mevcut Durum Analizi ile Risk Değerlendirmesi adımının birbirleri ile oldukça ilintili süreçler olduğu göz önünde bulundurulmalıdır.

Securitas Güvenlik Metodolojisi
İkinci Adım:

Güvenlik Hizmeti Risk Değerlendirmesi

Güvenlik Hizmeti Risk Değerlendirmesi

Risk belirsizliği ifade eden bir olasılıktır. Risk kavramı, kararların uygulanmasında sonuçlara ilişkin belirsizliği ortaya koyar. Bu açıdan bakıldığında risk, planlanan bir faaliyetin istenildiği şekilde gerçekleşmemesi veya istenmeyen bir olayın (ya da olayların) meydana gelmesi olasılığıdır.

> ***Büyük Larousse'a göre "risk" kavramının sözlük anlamı, bir zarara veya bir tehlikeye yol açabilecek bir olayın ortaya çıkma olasılığıdır.***

Bu noktada risk kavramı kaybetmenin nesnel beklentisi olarak ortaya çıkmaktadır. Buradaki kayıp bazen tesis ya da işletmede bulunan malzemeler (ör: bakır kablo, ofis malzemesi, değerli evrak/para, üretime ilişkin değerli malzeme, hammadde, vb.) olabileceği gibi bazı durumlarda itibar kaybı, bazı durumlarda ise can kaybı olarak karşımıza çıkar. Göz önünde bulundurmak gerekir ki; önemsiz olarak görülen, göz ardı edilen bir risk; tesis, tesis çalışanları ve hatta toplum için büyük olumsuzlukların başlamasına hatta önlenemez hasar ve krizlerin oluşmasına neden olabilmektedir. Bu nedenle büyük, orta, küçük ölçekli tüm tesislerde risklerin analiz edilerek her bir riskin değerlendirilmesi, korunan kurum stratejisi ve risk iştahı çerçevesinde öngörülen riskler için en uygun çözümlerin geliştirilmesi önem arz etmektedir. Bu süreç risklerin değerlen-

dirilmesi sürecidir. Risk değerlendirmesi en basit ifadeyle; tesis / organizasyonu etkileyecek potansiyel risklerin belirlenmesi, belirlenen bu risklerin gerçekleşme sıklıklarının ve gerçekleştiklerinde sebep olacakları etkinin büyüklüğünün tespit edilmesi ve kurumun risk iştahı[4] çerçevesinde belirlenen riskler için ihtiyaç duyulan çözümlerin geliştirilmesidir. Risk iştahı bir kavram olarak ilerleyen bölümlerde ele alınacak olmakla birlikte tespit edilen risklere alınacak tedbirlerin çerçevesinin belirlenmesi açısından önemli bir kavramdır. Risk değerlendirmesi ve bu değerlendirmeye göre alınacak tedbirler, tesisi ya da işletmenin risklerinin risk iştahı çerçevesinde kabul edilebilir sınırlara çekilmesi sürecinde oldukça kritiktir. Çünkü kurumun iş hedefleri ve stratejisi çerçevesinde değerlendirmeye alarak, kurum için kabul edilebilir sınırların üzerinde olan, gerçekleşmesi halinde kurumun öngördüğü ve kabul edebileceği sınırların üzerinde zarara / kayba neden olabilecek her bir risk kurumsal stres[5] kaynağına dönüşecektir. Stres bazen olumlu, bazen de yıkıcı etkileri olan bir kavramdır. Bu yönüyle güvenlik uygulamaları ve risk algısına bağlı olarak ortaya çıkan kurumsal stres yalnızca kurum yöneticileri ve çalışanlarını değil, kurum için hizmet üreten tedarikçilerin ve işletmenin diğer paydaşlarının da iş süreçlerini etkileyebilmektedir.

Örneğin; kurulum aşamasında bir fabrika düşünelim. Kurulum aşamasındaki bu fabrikanın şantiye sahasında birçok değerli malzeme bulunacaktır. Şantiye sahasından küçük tahta parçaları ya da küçük inşaat malzemelerinin kaybı / çalınması proje yönetim ekibi tarafından kabul edilebilir sınır olarak değerlendirilebilir. Ancak şantiye sahasında bulunan bakır kablo makaralarının çalınması kabul edilemez bir kayıp

---

[4] Kurumun bir katma değeri elde etmek için göze aldığı, başka bir değişle değer yaratırken kabul etmeye istekli olduğu risk miktarıdır.
[5] Kurumsal stres gerçekleştirilmesi gereken faaliyetler ile gerçekleşen faaliyetler arasında farklılık oluşmasına, bu farklılığında genellikle işletme veya tesisi olumsuz yönde etkilemesine neden olur. Bu durum kurumsal stres olarak adlandırılır.

olabilir. O halde bu şantiye yönetim ekibi için bakır kablo makaralarının çalınması risk iştahı üzerinde bir risk olduğu için bu kabloların çalınmaması için tedbir alması gerekir. Bu bakır kablo makaraları için bir tedbir alınmadığında bu risk algısı bir süre sonra bir stres kaynağına dönüşecektir. Yine aynı örnekte bir süre sonra değeri oldukça düşük bir bakır kablonun çalındığı düşünüldüğünde bu durumda risk iştahı üzerindeki riskin gerçekleşmiş olması kurumsal stres seviyesinin oldukça yükselmesine neden olacaktır. Bu durumda daha en başta kablo makaralarının çalınmaması için sadece bir kilit ve harici alarm sistemi gibi bir tedbir ile risk minimize edilebilecekken, küçük hırsızlık olayından sonra, kurumsal stres etkisi ile şantiye yönetimi tarafından ihtiyaç duyulandan daha fazla tedbir alınma yoluna gidilebilir. Bu durum kurumsal stres kavramının karar süreçlerine olumsuz etkisine örnek teşkil edecektir. Kurumsal Stres birçok farklı faktörün yanında risk algısına bağlı olarak da ortaya çıkabilir. İhtiyaç duyulan çözümler tespit edilerek bu çözümlerin uygulamaya alınması kurumsal stres kaynağını ortadan kaldıracaktır. Kurumsal stresin ortadan kaldırılarak kurum ikliminin iyileştirilmesi;

- Güçlü çalışan bağlılığı
- Verimlilik artışı
- Kurum kaynaklarının en doğru şekilde kullanımı
- Güvenli ve konforlu çalışma ortamı
- Kurum memnuniyeti

açısından önemli ve gereklidir.

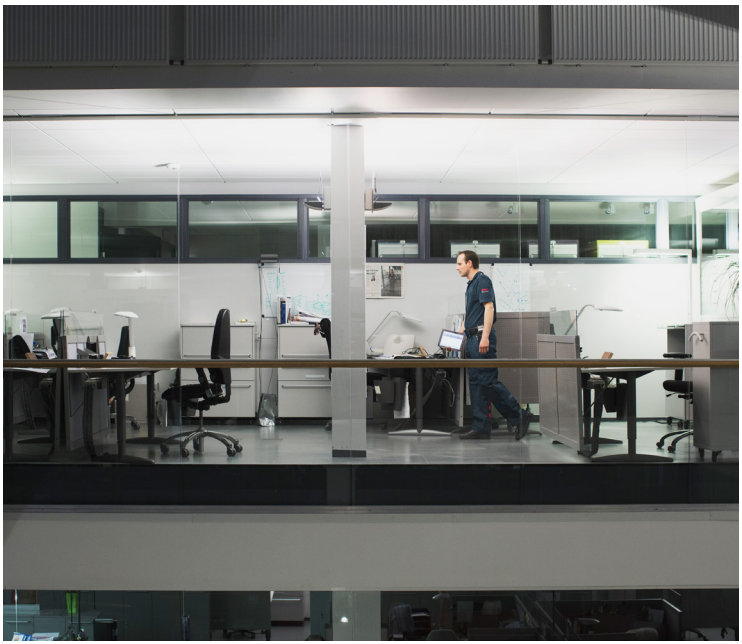
Kurumsal stres ile mücadele edebilmenin ilk adımı stres kaynağının ve olası etkilerinin tam olarak bilinmesidir. Kurumsal strese neden olan faktörlerden biri olarak güvenlik riskleri ancak risk değerlendirmesi ve bu değerlendirmeye göre alınacak aksiyonlar ile yönetilebilir.

Kurumu etkileyen tüm risklerin ortadan kaldırılması, sıfır risk ile kurum yaşamının sürdürülmesi gerçekçi bir beklenti değildir. Tedbir alınmasına gerek duyulmayan her bir risk,

gerçekleşme olasılığı, riskin potansiyel etkisi ve kurum iş stratejileri açısından kuruma olası etkileri göz önünde bulundurularak kabul edilmelidir.

Güvenlik faaliyetlerine odaklanan ve güvenlik risklerini ortaya çıkarmayı hedefleyen Güvenlik Hizmeti Risk Değerlendirmesi (GRD); güvenlik hizmeti verilecek olan tesis, bölge ve/veya yapılara yönelik potansiyel güvenlik tehditlerinin ve bu yapılarda mevcut güvenlik açıklarının tespit edilmesi sürecidir.

GRD Söz konusu tehdit ve güvenlik açıkları sonucunda oluşabilecek olası kayıpların (can, mal, itibar gibi) değerlendirilmesi ve bu bağlamda ortaya çıkan kabul edilemez risklerin belirlenmesidir.



Bu, kurum stratejilerinin oluşturulması ve uygulanması sürecinde önemli bir adımdır. Bu noktada kuruma etki edebilecek tüm risklerin tespit edilmesi, bu risklerin derecelendirilerek kurum için kabul edilemez risklerin belirlenmesi, risklerin gerçekleşmesine neden olacak senaryoların (Modus Operandi) belirlenmesi gerekir. Riskler bu şekilde doğru olarak tespit edilebilirse doğru çözümler ile karşılanabilir. Tespit edilemeyen riskler kurum için bir belirsizliktir. Güvenlik Risk Değerlendirmesi bir nevi tesisin faaliyetlerini sürdüreceği zemine ilişkin belirsizliğin ortadan kaldırılması gayretidir. Teknolojinin baş döndürücü bir hızla geliştiği ve rekabetin aynı oranda hızla şekillendiği bir ortamda, belirsizliğin işletmelere yükleyeceği stres oldukça büyük olacaktır. Kaotik ve karmaşık sonuçları olan belirsizlik, işletmeler açısından dikkat edilmesi ve sonlandırılması gereken bir durumdur. Güvenlik Risk Değerlendirmesi, güvenlik uygulamalarına ilişkin belirsizliklerin ve kurumsal stresin ortadan kaldırılması sürecinde en önemli araçtır.

Güvenlik Risk Değerlendirmesi, güvenlik uygulamalarına ilişkin belirsizliklerin ve kurumsal stresin ortadan kaldırılması sürecinde en önemli araçtır.

Bu noktada kurumsal stres nedir, etkileri nelerdir, açıklık getirilmesi fayda sağlayacaktır.

Kurumsal Stres Kavramı

Stres bir olay ya da durumun kişi ve/veya kurumlar üzerinde yarattığı etkidir. Başka bir deyişle stres, çeşitli çevresel faktörlere karşı gösterilen genel bir tepkidir. Stres, maddi ve manevi olarak zorlayıcı tehditler karşısında yeni bir uyum sağlama çabasına girilmesidir. Tıpkı bireylerde olduğu gibi kurumlar da maruz kaldıkları ya da maruz kalma potansiyeli taşıdıkları durum ve olaylara karşı bir takım reaksiyonlar geliştirirler. **Kurumu, rutinde davrandığından farklı davranmaya sevk eden faktörler kurumsal risk faktörleri olarak değerlendirilebilir.** Stresin hem bireyler hem de kurumlar için yalnızca olumsuz etkileri değil olumlu, güdüleyici etkileri de bulunmaktadır. Ölçülü stres motive edici, başarıyı arttırıcı etkiye sahiptir. Kurumsal stres ile güvenlik uygulamaları kapsamında yıkıcı etkiye sahip kurumsal stres kastedilmektedir.

> ***Kurumsal stres, gerçekleştirilmesi planlanan faaliyetler ile gerçekleşen faaliyetler arasında farklılık oluşmasına, bu farklılığın da genellikle işletme veya tesisi olumsuz yönde etkilemesine neden olur.***

Kurumsal stres kurum marka değeri, kurum varlıkları, çalışanlarının ve kurum paydaşlarının can ve mal güvenliğinin tehdit altında olabileceği algısı ile kurumun beklenen ve

hedeflenen fonksiyonlarından uzaklaşmasına da neden olabilir. Karar vericilerin kritik yol ayrımlarında aldıkları kararlar ile kurumun stratejileri dışında kararlar almasına, işletme yatırımlarını yanlış alanlara yönlendirmesine sebep olabilir. Kurumsal stres kavramının kurumların iş süreçleri üzerinde sebep oldukları olumsuz etkilerden bazıları şunlardır;

— Kurum içi iletişim ortamına zarar vermesi
— Çalışan performansında düşüşe neden olması
— Yüksek sirkülasyon oranına neden olması
— Karar vericilerin stratejik karar sürecini olumsuz yönde etkilemesidir.

Tüm bu etkiler, kurumun iş sürekliliğinin zarar görmesine ya da kurumun karlılık ve verimliliğinin düşmesine sebep olabilir.

Güvenlik uygulamaları kapsamında kurum üzerinde strese neden olabilecek güvenlik risklerinin bilinmesi, kurum risk iştahının tespiti ve güvenlik kurgusunun ve uygulamalarının bu farkındalık ile icrası önem arz eder. Bu farkındalık güvenlik açıkları ya da güvenlik risklerine ilişkin belirsizliğin neden olacağı stresi en aza indirecektir.

Risk iştahı çerçevesinde kabul edilebilir riskler bilinecek, kabul edilemez seviyedeki riskler için ise geliştirilecek çözümler belirlenecektir.

Kurumların Risk İştahı

Risk, modern yaşam koşullarında, tüm sektörel faaliyetler için büyük önemi olan bir kavramdır. Firmalar ve kurumlar hayatta kalabilmek için mal ve hizmet üretmeli, bu üretim süreçlerinde ortaya çıkan ya da ortaya çıkma potansiyeli taşıyan risklerle baş etmeli yani risklerini yönetmelidir. ***Risk yönetimi, örgütlerin kârlılıklarını devam ettirerek faaliyetlerini yürütmesini sağlayan, tesis açısından kıymetli olan can, mal, şöhret, kurumsal bilgi birikimi ve kurumsal tecrübe gibi maddi, manevi varlıkların korunması ile örgütlerin hayatına devam etmesine imkân tanıyan bir yönetim şeklidir.*** Risk yönetimi, oluşabilecek istenmeyen kayıpların kolay, hızlı ve en düşük maliyet ile engellenmesini sağlamaktadır. İstenmeyen kayıpların optimum yöntemlerle engellenebilmesi için potansiyel risklere karşı örgütlerin farklı çözüm yöntemleri üretme ihtiyacı doğmaktadır. Riskler, risklerin gerçekleşme sıklıkları ve gerçekleştiklerinde sebep olacakları kayıp; ilgili kurumun iş koluna, lokasyonuna, sahip olduğu çalışan sayısı ve iş hacmine göre farklılık gösterecektir. Bu nedenle farklı kurumlar için riskler aynı olsa bile risklerin sonucu farklılık gösterebilir. Bu doğrultuda kurumlar, riskleri kurum misyon ve vizyonu, politikası, ticari hedefleri, organizasyonel yapısı, faaliyet gösterilen sektörü, kurum ölçeği vb. faktörleri göz önünde bulundurarak önceliklendirir ve bu öncelik sırasına göre çözüm yolları geliştirmeye çalışır. Her tesis ya da organizasyonun karşı karşıya

kalabileceği riskler farklılık gösterdiği gibi, karşı karşıya kalınan riskleri kabullenme seviyeleri ve dolayısı ile risklere üretilen çözümler de birbirinden ayrışabilir. Bu kabullenme seviyeleri Risk iştahı olarak adlandırılır. ***Risk iştahı, kurumun bir katma değeri elde etmek için göze aldığı, başka bir deyişle değer yaratırken kabul etmeye istekli olduğu risk miktarıdır.*** Bir kurumun hiçbir risk almadan, risklerden kendisini tamamen arındırarak varlığını sürdürmesi gerçekçi ve makul değildir. Her kurum belli ölçüde riski kabul ederek faaliyetlerini yürütmek durumundadır. Ancak, kabul edilecek riskler ve risklerin büyüklüğü kurumdan kuruma değişiklik gösterebilir. Dolayısıyla her kurumun risk iştahı birbirinden farklı olacaktır. Bu noktada kurumların risk iştahının belirlenmesinde **"verimlilik"** ve/veya **"etkililik"** gibi kavramlar temel hareket noktası olmaktadır.

Kurumların risk iştahı birbirinden farklılık göstermektedir. Bu noktada kurumların risk iştahının belirlenmesinde "verimlilik" ve/veya "etkililik" gibi kavramlar temel hareket noktası olmaktadır.

Verimlilik, amaçlanan hedeflere ulaşılırken en az girdiyle en üst seviyede çıktı (ürün/hizmet) elde edilmesidir.

> ***Verimlilik, hedeflenen mal ve hizmetlerin üretilmesinde eldeki kaynakların yer ve zaman açısından mükemmel planlanmasını gerçekleştirerek en rasyonel yol ve yöntemlerle en ideal sonuçların elde edilmesini amaçlar.***

Bu yaklaşım risklerin ölçeklendirilmesi, derecelendirilmesi ve çözüm yollarının üretilmesi sürecinde; riskin gerçekleşmesi halinde neden olacağı kayıp büyüklüğü ile, çözümün sebep olacağı kaynak ihtiyacının verimlilik açısından değerlendirilmesi prensibidir. İşletmelerin bu yaklaşım ile alacağı çözüm kararı kurumun risk iştahı eşiğini oluşturan parametrelerden biridir.

Verimlilik ilkesi yanında kurumların risk iştahını etkileyen başka bir kavram ise güvenliğin etkililiği prensibidir. Kurumun içinde bulunduğu koşullar çerçevesinde belirlediği risk iştahı, güvenlik yapılanmasında etkililik ve verimlilik arasında bir denge kurmasını zorunlu kılar. Bazı kurumlar bulundukları

lokasyon, faaliyet gösterdikleri sektör, üretim türleri, kurumsal riskler ve kurum stratejileri nedeniyle daha güvenli tesisi ve daha güvenli bir kurum algısına ihtiyaç duyarlar. "Daha güvenli tesis / kurum algısı" oluşturma ihtiyacı güvenlik yapılanmasının etkililiğinin arttırılmasını gerektirir. Kimi durumlarda bu çaba verimlilik sınırlarını aşabilir. Böyle bir ihtiyacın bulunduğu ve risk seviyesinin yüksek olduğu; dolayısıyla etkili bir güvenlik kurgusu ve caydırıcı etkisi yüksek etkili bir güvenlik algısının zorunlu olduğu durumlarda, ilgili kurumun risk iştahı düşük seviyede kalacaktır. Yani risk alma kapasitesi sınırlı olacaktır. Bu hassasiyetteki kurumlarda, verimlilik sınırlarını aşan ancak etkili bir güvenlik yapılanması ihtiyacı öne çıkacaktır.

Kendi koşulları çerçevesinde risk iştahını belirleyen, bilen ve risklerini risk iştahı seviyesinde tutmayı başarabilen kurumlar; kesin olarak bilinemeyen ve tam olarak öngörülemeyen geleceğe ilişkin "makul bir güvence" oluştururlar.

Kurumun risk iştahının bilinmesi, kurum stratejisinin uygulanması, kurum kaynaklarının optimum şekilde yönetilebilmesi için büyük öneme sahiptir. Kurum kaynaklarından en yüksek verimin alınabilmesi, kaynakların kurum stratejisi ve risk iştahına uygun olarak kullanımı ile mümkün olabilecektir. Risk iştahına ilişkin farkındalık kurumun iş stratejilerine ilişkin kontrolsüz adım atması (gerçekçi olmayan cesaret) ile gereğinden fazla tedbirli olması arasında bir denge kuracaktır. Kaynakların, tedbir alınmasına ihtiyaç duyulmayan, kurum için kabul edilebilir risklerin minimize edilmesi için kullanılmasını engelleyecektir. Bu denge, kurumun istikrarı ve verimliliğinde önemli bir paya sahip olacaktır.

Kurum yönetimlerinin risk iştahı bilinmeden karar süreçlerini işletmeleri aşırı tedbirli olunması sonucunda kurumun

ölçeğini büyütme fırsatı verecek stratejik seviyede fırsatların kaçırılması ya da kaynakların ihtiyaç duyulmayan kabul edilebilir risk alanlarına kullanılması gibi sonuçlar doğurabilir. Aynı zamanda kurumu stratejik seviyede etkileyebilecek ve etkileri etraflıca incelenmeden kabul edilen risklerin gerçekleşmesi halinde iş süreçlerinin tahmin edilenden daha yüksek bir etki ile dramatik seviyede kötüye gitmesine neden olabilecek, kurum kaynaklarının israfına neden olabilecek sonuçlar da doğurabilir. Başka bir deyişle

Kurum Yönetimleri tarafından risk iştahının bilinmesi;

- ***Alınan kararların şeffaflığı,***
- ***Riske dayalı bütçelerin doğru yapılandırılabilmesi,***
- ***Onay sürecinin desteklenmesi,***
- ***Risk yükünün kontrol altına alması ve***
- ***İş sürekliliğinin sağlanmasına katkı sağlayacaktır.***

Risklerin belirlenmesi, ölçeklendirilmesi ve üretilecek çözümlerin tespiti her tesis/organizasyonun özel durumları göz önünde bulundurularak yönetilmesi gereken bir süreçtir.

Örneğin, bir akaryakıt işleme tesisinin karşı karşıya olduğu risklerle, bir e-ticaret firmasına ait deponun karşı karşıya olduğu riskler farklılık gösterecektir. Yine iki akaryakıt tesisinin riskleri farklılık gösterebileceği gibi risk kabul seviyeleri de (risk iştahları) birbirinden farklı olabilir. Örneğin A akaryakıt işleme tesisi için hırsızlık ve terör eylemi riski kabul edilemez bir risk iken, B akaryakıt işleme tesisi için terör eylemi riski kabul edilemez bir risk; ancak, hırsızlık kabul edilebilir bir risk olarak konumlandırılabilir. Bu bilgiye göre A akaryakıt tesisi risk iştahı düşük, B akaryakıt tesisi ise A'ya göre risk iştahı yüksek bir tesistir.

Bütüncül Risk Yaklaşımı

Risklerin bir bütün olarak ele alınması ve aşağıdaki hususların hesaba katılması bir işletmenin risklerinin doğru belirlenmesi aynı zamanda risklerin gerçekleşme sıklığı ve etkilerinin doğru tespiti için son derece önemlidir.

— Güvenlik açıklarının birbirleriyle etkileşiminin,
— Teknolojide yaşanan güncel gelişmelerin tesis için potansiyel risklere, risklerin gerçekleşme sıklığı ve gerçekleştiğinde yaratacağı sonuca etkisinin,
— Segmente özgü risk haritası ve risk geçmişinin

hesaba katılması; risklerin, risklerin gerçekleşme sıklığı ve olası etkilerinin doğru tespit edilebilmesi için son derece önemlidir. Bu yaklaşım, kurumun risk iştahı ve olası güvenlik yatırımlarını da doğrudan etkileyebilecek bir yaklaşımdır.

Risk Etkileşimi

Bazı güvenlik açıkları tek başlarına değerlendirildiğinde kurum için düşük önem seviyesinde olup kabul edilebilir bir risk olarak görülebilecekken, yine bu şekilde düşük önem seviyesinde ve kabul edilebilir başka risklerle birleştiğinde; işletme için kabul edilemez sınırlarda bir güvenlik riskine dönüşebilir.

Bu nedenle tesis / organizasyon riskleri değerlendirilirken risklerin birbirleriyle olası etkileşimlerinin de hesaba katılması gerekir. Bir güvenlik riskinin başka bir riskin tetikleyicisi olup olmayacağı ya da düşük önem düzeyinde görülen bir güvenlik açığının başka bir güvenlik açığı ile birleşerek çok önemli bir riskin gerçekleşmesine zemin hazırlayıp hazırlamayacağı göz önünde bulundurulmalıdır.

Örneğin, çevre hattında 150 adet güvenlik kamerası bulunan bir tesiste, kameralardan birinin görüntü kalitesinin düşük ve yerleştirilme açısının uygun olmaması kabul edilebilir bir güvenlik açığı olarak düşünülebilir. Aynı şekilde söz konusu tesiste idari bina acil çıkış kapılarından birinin arızalı olması ve dışarıdan içeriye kontrolsüz geçişe imkân veriyor olması da kabul edilebilir bir açık olarak değerlendirilebilir. Ancak bu iki güvenlik açığı birleştiğinde tesis için kabul edilemeyecek risk olan hırsızlık, sabotaj gibi eylemlerin gerçekleşmesine zemin hazırlayabilir. Tesisin çevre hattında bulunan görüntüsü yetersiz kameranın bulunduğu alandan kabul edilebilir risk olan “mülke izinsiz giriş riski” gerçekleşmesi tek başına bakıldığında bir işletme için kabul edilebilir olarak değerlendirilebilir. Ancak bu mülke izinsiz giriş riski, arızalı acil çıkış kapısından idari bina ve yönetim katına erişim ile birleştiğinde işletme için kabul edilemeyecek olan “hırsızlık”, “sabotaj” veya “asayiş” gibi önemli risklere zemin hazırlayabilir. Bu nedenle, tesis ya da organizasyonların riskleri değerlendirilirken bütüncül bir bakış açısı ile değerlendirilmesi ve bu kapsamda;

- Potansiyel risklerin birbirlerine olan etkisi
- Risklerin gerçekleşmesine zemin hazırlayan senaryoların birbirleri ile etkileşimi
- Güvenlik açıklarının birbirlerini tetikleyici ya da etkisini arttırıcı potansiyellerinin

bilinmesi ve hesaba katılması daha doğru bir risk değerlendirmesi ve yönetimi için fayda sağlayacaktır. Bu bakış açısı gösteriyor ki;

Kurumların risk iştahının ve buna bağlı olarak güvenlik yapılanması ile bütçesinin belirlenmesi süreci risklerin listelenmesi, derecelendirilmesi ve bu derecelendirmeye göre aksiyon alınmasından daha karmaşık, çok yönlü ve sistematik bir yaklaşımı zorunlu kılar.

Bütüncül risk yaklaşımı çerçevesinde göz önünde bulundurulması gereken başka bir husus ise teknolojinin kurum risklerine olan etkisidir.

Güvenlik Risklerine Teknoloji Etkisi

Günümüz teknoloji dünyasında yaşanan hızlı değişim ve dönüşüm güvenlik uygulamalarını da doğrudan etkilemektedir. Teknolojik her yenilik, kurumlara güvenlik yapılanmasını oluştururken yeni fırsatlar sunduğu gibi yeni güvenlik risklerinin ortaya çıkmasına ya da mevcut risklerin potansiyel etkisinin katlanarak artmasına da sebep olmaktadır. Bu nedenle işletmelerin güvenlik profesyonelleri ya da hizmet üreten özel güvenlik şirketleri güvenlik teknolojileri dünyasında yaşanan gelişmeleri yakından takip etmeli; teknolojinin potansiyel risklere olan etkisi ve çözümlere teknolojiyi yansıtma imkânını daima göz önünde bulundurmalıdır.

Örneğin, endüstriyel tesisler ve savunma sanayi tesisleri için sabotaj son derece önemli ve potansiyel etkisi yüksek bir risktir. Günümüz koşullarında bu riskin gerçekleşme yolları senaryo arasına drone ile sabotaj ihtimali eklenmiştir. Bu çerçevede, kurumlar için olası risk ve bu riskin etkisini azaltmaya katkı sağlayacak teknolojik çözümler ilgili gelişme ile bütüncül şekilde ele alınmalıdır. Hatta bu teknoloji ve çözümlerin ilgili yasalar çerçevesinde kullanımına ilişkin kamuoyu farkındalığı oluşturulması da konunun çok önemli yönlerinden biridir.

Bu noktada kurumların güvenlik hizmeti aldığı güvenlik şirketlerinin ve/veya kurum bünyesinde bulunan güvenlik profesyonellerinin fonksiyonları nedir?

Tesis / işletme yönetimleri, kurum stratejileri ve hedeflerini belirlerken riskleri en aza indirebilmek ya da ortadan kaldırabilmek için;

— Kurum risk iştahı seviyesi (kabul edilebilir ve kabul edilemez risklerin belirlenmesi)
— Güvenlik hizmeti yapılandırılırken verimliliğin mi etkililiğin mi ön planda tutulacağı
— Güvenlik ihtiyaçlarına ilişkin öncelikli ve gerekli yatırımların tespiti

konularında hizmet alınan güvenlik şirketi ya da kurum bünyesinde bulunan güvenlik profesyonellerinin danışmanlığına / yönlendirmesine ihtiyaç duyarlar. Güvenlik şirketleri ve güvenlik profesyonelleri tarafından yapılacak bu danışmanlık ve yönlendirme faaliyetinin temeli risk analizine dayanır. Bu kapsamda risk analizinin gerçekleştirilmesi için;

— Risklerin tespit edilmesi,
— Risklerin önceliklendirilmesi,
— Kurum kaynakları, stratejisi ve iş planlarına en uygun çözümün tespit edilmesi,
— Çözümün uygulanması,
— Takip ve kontrol faaliyetlerinin gerçekleştirilmesi gerekir.

Risk analizi faaliyetinin;

— Güvenlik hizmetinin yapılandırılma aşamasında,
— Yapısal bir değişim meydana geldiğinde,
— Bir olay yaşandığında,
— Her halükârda belirlenen bir periyot dahilinde yenilenmesi önem arz eder.

Risk analizinin doğru sonuçların elde edilebilmesi için doğru esaslarla uygulanması gerekir.

Risk Analizi Uygulama Esasları

Risk Analizi, dahili ve/veya harici güvenlik açıklarına bağlı olarak güvenliği ihlal eden bir olayın soygun, sabotaj, yangın vb. olayların gerçekleşme olasılığının ve yaratacağı olası sonuçların ölçümüdür.

Güvenlik Hizmeti Risk Değerlendirmesi ise belirli bir senaryo için yangın, soygun, sabotaj vb. olayların oluşabilecek risklerin belirlenmesi sürecidir.

Güvenlik Hizmeti Risk Değerlendirmesi yapılırken saldırganın hareket tarzı ya da olayın gerçekleşme şekli (Modus operandi / senaryo) dikkate alınır. Bir senaryo üç temel soruya cevap verir. Bu sorular:

— Nerede?
— Ne zaman?
— Nasıl?'dır.

Örneğin; bir mağazaya yönelik gerçekleştirilebilecek soygun girişimi (Senaryo) tanımlanırken nerede (ana giriş kapısından), ne zaman (gece yarısı) ve nasıl (kapı penceresini kırarak) soruları cevaplanır.


Securitas

Güvenlik Hizmeti Risk Değerlendirmesi iki temel adımda yapılır. Bunlar:

— Tehditlerin (Senaryo) analiz edilmesi
— Olayın gerçekleşme olasılığı ile etkisinin yani yol açacağı maliyetin/zararın büyüklüğünün etkileşimi sonucunda riskin tanımlanmasıdır.

Güvenlik Hizmeti Risk Değerlendirmesi bir sonraki adımda kuruma özel çözümlerin üretilebilmesi için yürütülmesi elzem bir süreçtir. MDA ile elde edilen bilgiler Güvenlik Hizmeti Risk Değerlendirmesi yapılırken kullanılır. Bir sonraki adımda ise tespit edilen her bir riski karşılayan ve Kuruma özel güvenlik çözümleri üretilir.

"Güvenlik Hizmeti Risk Değerlendirmesi" yapılırken aşağıdaki konular dikkate alınır:

1. Güvenlik Hizmeti Risk Değerlendirmesinde, önce "Mevcut Durum Analizi"nde saptanan hizmet yeri ve segment yapısı esas alınır.
2. Güvenlik Hizmeti Risk Değerlendirmesi yapılırken kurumsal hafıza ve segmente özel risk ve çözümleri referans olarak çıkarabilen Securitas Smart Risk Analizi (SRA) kullanılır.
3. Güvenlik Hizmeti Risk Değerlendirmesi proje/birim bünyesinde bulunan ve risk ihtiva eden her bir hizmet yeri için yapılır. Bu hizmet yerleri risk analizini gerçekleştiren güvenlik profesyoneli (Güvenlik Hizmeti Risk Değerlendirmesine katılan personelin desteğiyle) tarafından olası riskler açısından bir bir incelenir.
4. Yeni gelişen durumlara bağlı olarak belirtilen risklerin haricinde farklı riskler tespit edildiğinde bunlar da değerlendirmeye tabi tutulur.
5. Güvenlik Hizmeti Risk Değerlendirmesi aşağıdaki sıra takip edilerek yapılır:
    a. Risk/riskler belirlenir.
    b. Her bir risk için olasılık ve etki katsayıları belirlenir.
    c. Her bir riskin senaryo saptanır.

d. Her bir risk için belirlenmiş olan olasılık değeri ile etki değeri çarpılarak bir risk katsayısı bulunur.
e. Tesis için bir risk matrisi oluşturulur.

6. Hizmet yerini oluşturan bütün alanlar (nizamiye, ortak alanlar, merdivenler, otopark vb.) incelenir. Her bir alanda oluşabilecek riskler (soygun, yangın, izinsiz giriş vb.) tespit edilir ve her bir risk için olasılık ve etki katsayıları belirlenir. Olasılık düzeyleri sırasıyla; düşük (1), orta (2), yüksek (3) ve çok yüksektir (4).
   a. Düşük (1) olasılık, tehdidin on yılda bir kez ya da daha az gerçekleşme sıklığına karşılık gelmektedir.
   b. Orta (2) olasılık, tehdidin son birkaç yılda bir kez gerçekleşme sıklığına karşılık gelmektedir.
   c. Yüksek (3) olasılık, tehdidin yılda en az bir kez gerçekleşme sıklığına karşılık gelmektedir.
   d. Çok yüksek (4) olasılık ise tehdidin ayda en az bir kez gerçekleşme sıklığına karşılık gelmektedir.
7. Projede güvenlik hizmeti sağlanacak olan tesis yeni kurulmuş olabilir. Böyle bir durumda yalnızca söz konusu tesis ya da işletmenin risk geçmişi değil, faaliyet gösterilen segmente ve/veya lokasyona özgü ortalama risk geçmişinin göz önünde bulundurulması risklerin gerçekleşme olasılığının daha doğru saptanmasına katkı sağlayacaktır.
8. Her bir riskin etkisi (gerçekleşmesi halinde yol açacağı zararlar) tespit edilirken, etkiler sırasıyla düşük (1), orta (2), yüksek (3) ve çok yüksek (4) olmak üzere derecelendirilir.
   a. Düşük etki (zarar); hafif yaralanmalar, düşük ölçekli finansal kayıplar ve üretimin geçici olarak sekteye uğramasına karşılık gelmektedir.
   b. Orta düzeyli etki; hizmet kalitesinde kısmi azalma, yaralanmalar, yüksek restorasyon/tamirat masrafları ve diğer finansal kayıplar, sınırlı hizmet sunumunda devamlılık durumlarına karşılık gelmektedir.

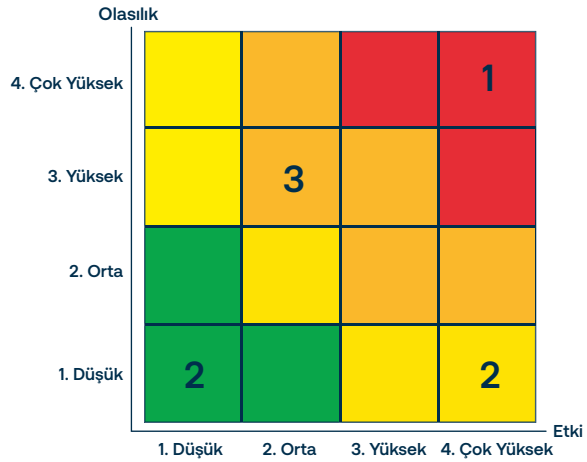
Risk geçmişinin göz önünde bulundurulması risk gerçekleşme olasılığında etkilidir.

c. Yüksek düzeyli etki; servis kalitesinde sürekli düşüklük, önemli ve çok sayıda yaralanma ve büyük ölçekli finansal kayıpların yaşandığı durumlara karşılık gelmektedir.

d. Çok yüksek düzeyli etki ise itibar kaybı, ölümlü kazalar ve olaylar, çok büyük finansal kayıplar, hizmet sunumunda önemli kesintiler ve kopuklukların yaşandığı durumlara karşılık gelmektedir.

Her bir risk için olasılık ve etki katsayıları belirlendikten sonra müşteri ile mutabakat sağlanarak kabul edilemeyecek riskler üzerinde anlaşma sağlanır.

Her bir risk için olasılık ve etki katsayıları belirlendikten sonra müşteri ile mutabakat sağlanarak kabul edilemeyecek riskler üzerinde anlaşma sağlanır. Bu riskler çözüm geliştirilecek risklerdir.



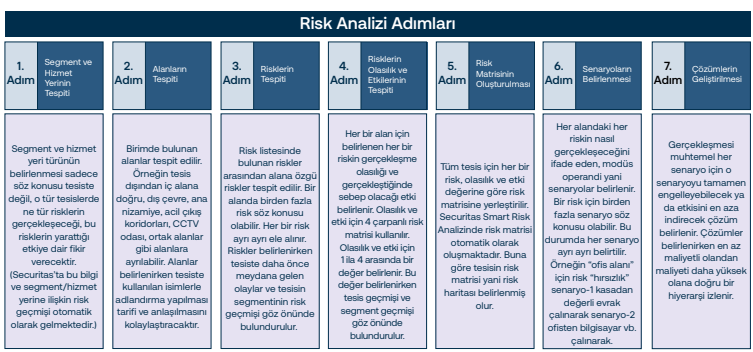
Tablo 1. Risk Önem Dereceleri

Renk	Risk Katsayısı	Risk Etki Derecesi
Yeşil	1-2	Düşük
Sarı	3-4	Orta
Turuncu	6-9	Yüksek
Kırmızı	12-16	Çok Yüksek

Tesis için risk matrisi oluşturulduktan sonra aşağıda yer alan tablo hazırlanarak riskler önem derecesine göre sıralanır.

Risk Önem Derecesi	Riskler**	Risk Olasılık Derecesi	Risk Etki Derecesi	Risk Katsayısı	Bölgeler*
Çok Yüksek	Risk A	4	4	16	Bölge 1
Yüksek	Risk B	3	3	9	Bölge 2
	Risk C			9	Bölge 3
	Risk D			9	Bölge 3
Orta	Risk E			4	Bölge 1
	Risk F			4	Bölge 3
Düşük	Risk G			1	Bölge 4
	Risk H			1	Bölge 2

9. Sonrasında her bir riskin “Senaryo” belirtilir. Yani, o riskin nerede, ne zaman ve nasıl gerçekleşebileceğine ilişkin düşünceler açıklanır. Senaryo projeye ve hizmet yerine bağlı olarak değişiklik gösterebilir.
10. Her bir riske karşılık olarak halihazırda alınmış olan bir güvenlik tedbirinin olup olmadığı tespit edilir. Riskin gerçekleşebileceği yerin fotoğrafları çekilir ve varsa ilave notlar eklenir.
11. Bu işlemlerin sonunda risk tanımlaması yapılırken, her bir risk için belirlenmiş olan olasılık değeri ile etki değeri çarpılarak bir risk katsayısı bulunur ve tesis için bir risk matrisi oluşturulur. Oluşturulan risk matrisinde; risk katsayısı 2 ve daha düşük olan riskler düşük öneme sahip riskler, risk katsayısı 3 ve 4’e eşit olan riskler orta derece öneme sahip riskler, risk katsayısı 6, 8 ve 9 olan riskler yüksek öneme sahip riskler, risk katsayısı 12 ve 16 olan riskler ise çok yüksek öneme sahip riskler şeklinde derecelendirilir.



Securitas Güvenlik Metodolojisi
Üçüncü Adım:

Çözümler

Çözümler

a. Genel Esaslar

Bu adım Kurumun güvenlik hizmetine ilişkin talepleri doğrultusunda ve mevcut durum analizi ile elde edilen bilgiler ışığında bir önceki adımda belirlenmiş olan riskleri azaltacak entegre güvenlik çözümlerinin geliştirilmesi ve Kuruma sunulması adımıdır.

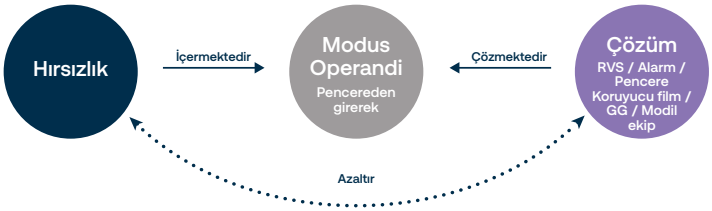
Securitas'ın çözüm üretme yaklaşımı pazardaki rakipler karşısında rekabetçi avantaj elde edilmesinde önemli bir rol oynamaktadır.

Securitas'ta güvenlik çözümleri üretilirken temel yaklaşım, üretilen çözümün riskleri karşılaması ve azaltmasıdır. Bu nedenle temeline riski alan çözümler, çözüm üretme adımının esasını oluşturmaktadır.

İnsanlı güvenlik hizmetinin mobil koruma, elektronik güvenlik, uzaktan koruma, profesyonel risk analizi ve diğer gelişmiş, ileri teknolojili koruyucu hizmetlerle desteklenmesi suretiyle "Entegre Güvenlik Çözümleri"nin geliştirilmesi sağlanır. Güvenlik çözümü tasarlarken; Uzman Güvenlik Hizmetleri, Güvenlik Teknolojileri, Uzaktan İzleme Hizmetleri, Kontrol Hizmetleri, İtfaiye Hizmetleri ve Güvenlik Danışmanlığı çözümlerinin bir araya getirilmesiyle ortaya çıkan, ilgili kurumun güvenlik ihtiyaçlarını daha etkin, daha verimli ve daha ekonomik şartlarda karşılayan optimum çözüme Entegre Güvenlik Çözümleri (EGÇ) denir. Securitas, Entegre güvenlik çözümlerinin sağladığı optimizasyon Kuruma sunulan güvenlik hizmetinin etkinliğini arttırırken maliyet avantajı sağlamayı hedefler.

Risk değerlendirme süreci sonunda her bir hizmet yeri için derecelendirilen ve tanımlanan risklerin, üretilen güvenlik çözümleriyle tamamen ortadan kaldırılması ya da etkisinin sınırlandırılması hedeflenir. Bu yaklaşım aşağıdaki şekilde gösterilmiştir.

Örneğin, pencereden girmek suretiyle gerçekleşebilecek hırsızlık tehdidi bir risk oluşturmakta ve üretilen çözüm (video analiz özellikli kamera kurulumu, alarm sistemi kurulumu, pencereye koruyucu film çekilmesi, güvenlik görevlisi görevlendirilmesi, mobil ekip görevlendirilmesi vb.) bu tehdidi birebir karşılayarak risk katsayısını düşürmektedir.



Güvenlik çözümleri oluşturulurken dikkate alınacak yaklaşım risklere karşı önleyici tedbir alınması, riskin teyit edilmesi ve müdahale edilmesidir.

Örneğin, binanın zemin katında bulunan pencerelerden gece saatlerinde yapılabilecek hırsızlık girişimine karşı video analiz özellikli kamera sisteminin kurulması bir tedbirdir. Hırsızlık girişiminde bulunulması halinde aktif hale gelen alarm sonucunda görüntülerin incelenmesi, teyit ve bunun karışlığında sesli ikazda bulunulması ve mobil ekiplerin bölgeye yönlendirilmesi ise hırsızlık girişiminde bulunan kişiye müdahale etmektir (doğrulama / müdahale).

b. Optimizasyon:

Optimizasyon; mümkün olan en az maliyetle en verimli çıktının elde edilmesi için uygulanan yöntemler bütünüdür. Bu bakış açısı ile kurum kaynaklarının en doğru şekilde kullanılabilmesi için riskleri ortadan kaldıracak ya da etkisini en aza indirecek çözümün optimizasyonu büyük önem taşır.

Çözümün oluşturulması aşamasında belirlenen ve ölçeklendirilen riskler arasından gerçekleşme olasılığı en yüksek olan ve gerçekleştiğinde de en büyük etkiyi yaratacak yani kurum için öncelikli risklerin çözümüne öncelik verilir. Geliştirilecek çözümler ile bu risklerin etkisinin tamamen ortadan kaldırılması ya da etkisinin sınırlandırılması hedeflenir. Dikkat edilmesi gereken bir diğer husus ise kurum kaynaklarının en doğru şekilde kullanımı için geliştirilecek çözümün optimize edilmesidir. Bu şekilde sağlanacak optimizasyon, riski karşılayacak yeterlilikte ve olabilecek en düşük maliyette çözümün uygulanmasıdır. Bu kapsamda aşağıdaki hususlar dikkate alınır.

- Her bir risk için çözüm üretilirken belirli bir öncelik sırası takip edilir. Bu öncelik sırasına göre riskin etkisinin ortadan kaldırılması ya da etkisinin azaltılması gayreti kurum kaynaklarının en doğru şekilde kullanılmasına da hizmet eder. Bu sıra aynı zamanda risk azaltma (mitigation) planı olarak da tanımlanmaktadır.
- Riskleri karşılayan çözümler üretilirken ilk olarak üretilen çözümün riski karşılayabilecek yeterlilikte olmasına dikkat edilir. Ardından riski karşılayacak çözümler arasında daha düşük maliyetli olandan maliyeti yüksek olana doğru bir hiyerarşi izlenir. Düşük maliyetli çözümün riski karşılamakta yetersiz kalacağının değerlendirilmesi halinde sadece bir üst basamaktaki çözüm beraber değerlendirilir. Bu hiyerarşi tesis, hizmet yeri ya da riske göre değişkenlik göstermekle birlikte aşağıdaki şekilde uygulanabilir.

Tedbirlerin Maliyet/fayda hiyerarşisi aşağıdaki gibidir.

1. **Prosedür ve kuralların belirlenmesi:** Tesis ve işletmeler için en temel tedbirler, kuralların belirlenmesi, çalışan ve ziyaretçilere duyurulması ve uyulmasının sağlanması ile alınır. Tesisin yaşam kuralları olası riskleri azaltacak ve tesis verimliliğini arttıracak şe-

kilde belirlenir. Kuralların belirlenmesi ve uyulması en düşük maliyetli – hatta maliyetsiz tedbirlerdir. Çoğu zaman detaylı olarak düşünülmüş ve titizlikle uygulanan talimat ve kurallar riskler açısından önleyici, sınırlandırıcı ve caydırıcı etkiye de sahiptir.

Örneğin gün içinde havalandırma amacıyla açık bırakılan ofis camları mesai bittikten sonra bir zafiyete dönüşür. Bu camlara demir parmaklık takılması bir fiziki tedbirdir. Ancak güvenlik ekibine mesai biter bitmez bu camların kontrolünü sağlayıp, açık camların kapatılması yönünde bir talimat verilmesi ve bunun titizlikle uygulanması da etkili bir çözümdür. Açık bırakılan camdan giriş senaryosu ile gerçekleşecek "mülke izinsiz giriş ve/veya hırsızlık" gibi risklerin olasılık ve etkisini düşürecektir. Düzenli olarak yapılan bu güvenlik kontrolü aynı zamanda birçok güvenlik riski için de caydırıcı etkiye sahiptir. Bu nedenle bir prosedür ya da kural koyulup, bu kurala uyulmasının sağlanması ile bir risk ortadan kaldırılabilecek ise bu uygulama o risk için en optimum çözüm olacaktır.

2. **Fiziki tedbirlerin alınması:** Belirlenen kuralların sonrasında bir dizi fiziksel tedbir alınması gerekebilir. Bazı risklerin engellenmesi için prosedür ve kuralları fiziki tedbirler ile desteklenmesi gerebilir. Çevre duvarları ve/veya tel çitler, değişik özelliklere sahip kapılar, kilitler, zor kırılan camlar vb fiziki tedbirlere bazı örneklerdir. Fiziksel tedbir amacıyla kullanılan bu tür ekipman ve malzemenin ömrü uzun, hasar görmesi daha zor ve amortisman süreleri fazladır. Bu nedenle yıllık/aylık maliyetleri oldukça düşüktür.
3. **Teknolojik çözümlerin kullanılması:** Fiziki tedbirlerin sonrasında erişim kontrol için kartlı veya biyo-

metrik geçiş kontrol sistemleri, algılama için farklı amaçlarla kullanılan dedektörler (gaz, hareket, yangın vb) veya analiz kabiliyeti olan kameralar kullanılır. Bu teknolojik çözümlerin de kullanım ömrü oldukça uzundur, teknolojilerine bağlı olarak alarm sistemleri ve dedektörler on yıla yakın verimli çalışabilmekte, kamera sistemleri de beş ila sekiz yılda amorti olmaktadır. Teknolojik çözümler kurum verimliliğine önemli katkı sağlayan araçlardır.

4. **Uzaktan izleme/müdahale hizmetlerinin verilmesi,** Yukarıda belirtilen teknolojiler uzaktan izleme merkezlerine sinyal ve bilgi yollayarak doğrulama ve müdahale imkânı vermektedir. Uzaktan izleme merkezlerine uzman operatörler alarm dedektörlerinden gelen sinyalleri veya analiz yeteneği olan kameralardan gelen görüntüleri yorumlayarak tehdidi doğrulayabilmekte ve uygun teknolojiler mevcut ise uzaktan sesli veya cihazlar aracılığı ile müdahale edebilmektedirler. Teknolojilerin uzaktan izlenebilmesi ve gerektiğinde müdahale edilmesi tesis içinde daimî güvenlik görevlileri bulundurulmasından daha az maliyetli bir çözümdür. Ayrıca uzaktan kontrol, sanal devriye vb. gibi faaliyetlerle kurum güvenliğinin etkinliğinin artmasına önemli ölçüde katkı sağlayan çözüm ve sistemlerdir.
5. **Mobil Devriye (Kontrol) hizmetlerinin verilmesi** Yukarıda alınan tedbirlerin riskine ve müdahale yöntemlerine bağlı olarak yerinde doğrulama ve müdahale için tesis içindeki veya bölgedeki devriye güvenlik görevlileri uzaktan izleme merkezleri ile irtibatlı olarak gelen sinyallerin hem doğrulamasını sağlayabilir ve hem de yetkinlik, eğitim ve donanımlarına bağlı olarak müdahale edebilirler. Bu tedbir insan kaynağı içerdiği için önceki tedbirlerden daha

maliyetli olmakla birlikte daimî güvenlik görevlisi bulundurulmasına oranla daha az maliyetlidir ve risk ile müdahale yöntemi bu tedbirlerin alınması gerekli kılabilir.

6. **Daimî Güvenlik Görevlisi görevlendirilmesi:** Yukarıda belirtilen tedbirlerin bir kısmı veya hepsi alınmasına rağmen risk ve müdahalenin gereği daimî olarak bir güvenlik görevlisinin bulundurulması gerekebilir. Daimî olarak bir güvenlik görevlisinin bulundurulması değişken durumların değerlendirilmesi, kişiler ile iletişim kurulması, kişilere karşı yerinde hızlı müdahale gerektirmesi, erişimin fiilen bir insan tarafından kontrol edilmesi gibi gerekliliklerin oluşması halinde gerekebilir. Daimî bir güvenlik görevlisi görevlendirilmesi hem en maliyetli hem de performansı tutarlı olmayan bir çözüm olabilir.

Bu yaklaşım çözümlerin optimizasyonunu sağlayan bir yöntemdir.

— Çözümler optimize edilirken, kurum kaynaklarını en etkili şekilde kullanabilmek için düşük maliyetli ve en uygun çözüm bileşenlerinden başlayarak çözüm paketleri belirlenir. Bu bakış açısı ile insanlı güvenlik çözümlerinin üretilmesi son aşamada yer almaktadır. Çünkü insanlı hizmet sürekli devam edecek ücret maliyeti, vergi yükümlülükleri, idari ve operasyonel gereklilikler gibi nedenlerle en maliyetli çözüm yöntemlerinden biridir. Bariyer, kapan, tel çit vb. fiziksel çözümler ile; kamera, alarm sistemi vb. gibi teknolojik çözümlerde ise bu maliyetler daha düşüktür. Bu ürünlerin de kurulum maliyetleri, ürüne göre değişecek süre ile devam edecek amortisman ve bakım maliyetleri bulunmaktadır. Prosedür ve kural değişikliği ile bir riskin karşılanabilecek olması halinde, fiziksel, teknolojik tedbir ya da güvenlik

görevlisi görevlendirmek yerine bu alternatifin seçilmesi en uygun çözüm olacaktır. Çünkü prosedür ve kural değişikliği yöntemi en düşük maliyetli çözüm paketidir.

— Optimizasyonda amaç yalnızca maliyetlerin azaltılmasının ötesinde, riski karşılayabilecek yeterlilikte en düşük maliyetin hedeflenmesidir. Geliştirilen çözüm riski karşılayabilecek yeterlilikte olmalıdır. Bu da bazı durumlar için birden fazla çözüm grubunun bir arada kullanılmasını gerektirebilir.
— Optimizasyon sürecinde öncelikle etkili ve düşük maliyetli çözüm araçları risk azaltma planına dahil edilir. Risk katsayısına bağlı olarak birden çok tedbir bir arada uygulanarak riskin azaltılması (mitigation) pekiştirilebilir. Bu nedenle üretilen çözümlerin salt insanlı ve fiziki tedbirlerin alındığı bir güvenlik hizmeti olmasının ötesinde, Entegre Güvenlik Çözümleri (EGÇ) kategorisinde yer almasına çalışılır. Bunun anlamı, riski ortadan kaldıracak ya da etkisini azaltacak çözümler arasında fiziki güvenlik tedbirleri ve güvenlik görevlisi çözümünün yanında teknoloji, mobil hizmetler ve uzaktan izleme gibi seçeneklerin de değerlendirilmesidir
— Alınan tedbirlerin uzun dönemli (örneğin beş yıllık) maliyetleri ilgili kuruluş ile paylaşıldığında hangi risklerin nasıl bir maliyet ile azaltıldığı ortaya çıkacaktır. Önerilen tedbirlerin maliyetleri berraklaştığında ilgili kuruluşun risk iştahında değişiklikler olabilir, baz maliyetlere katlanmayarak daha fazla risk alma eğilimi ortaya çıkabilir. Bu karar sürecinde vazgeçilen çözümün maliyeti ve bu çözümden vazgeçilmesine bağlı olarak gerçekleşebilecek riskin olası maliyetine ilişkin bir tahmin oluşturulur. Bu bilgi ışığında, vazgeçilen tedbir ve buna bağlı olarak maruz kalınabilecek riskler ve sonuçları ilgili kurum ile paylaşılır.

— Bu süreç tamamlandığında başlangıçta öngörülen kabul edilebilir riskler değişmiş olabilir. Bu aşamada hangi risklerin hangi tedbirler ile kapatılabildiği veya azaltılabildiği yazılı olarak belirtilip anlaşmaya varılarak uygulamaya geçilir.

c. Çözüm Hiyerarşisi

Özel güvenlik faaliyetlerinin temel amaçlarından biri istenmeyen bir olay meydana gelmeden önce olayın gerçekleşmesini engellemek, oluşturulan güvenli alan algısı ile kötü niyetli kişileri caydırmak ve potansiyel tehlikelerin gerçekleşmesini önlemektedir. Gerçekleşmesi engellenemeyecek güvenlik olayları için de etkilerinin mümkün olduğunca sınırlandırılması hedeflenir. Ancak caydırma gayretinin yetersiz kaldığı ve bir olayın meydana geldiği durumlarda aşamalı olarak durumun algılanması, doğrulanması, müdahale gerçekleşinceye kadar geciktirilmesi ve müdahale edilmesi gerekliliği ortaya çıkar. Tüm bu faaliyetlerinin doğru şekilde yürütülebilmesi;

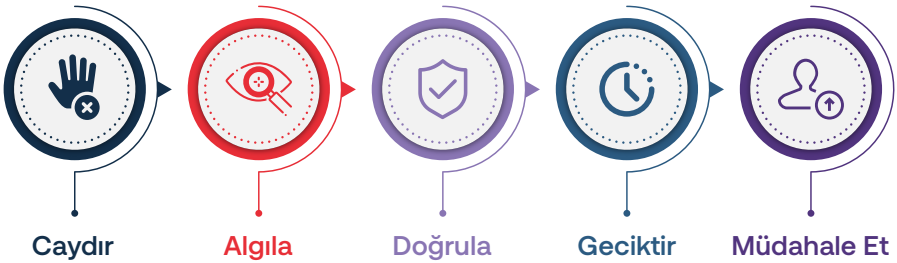
Riskleri minimize etmek ya da tamamen ortadan kaldırmak için önerilen çözümler bu 5 adıma cevap verecek nitelikte dizayn edilmelidir.

— İlgili kanunların özel güvenlik görevlilerine verdiği yetki ve sorumlulukların yerine getirilmesi,
— Hizmet verilen yerlerdeki paydaşların can ve mal güvenliğinin etkin şekilde sağlanması,
— Güvenlik ekibinin can güvenliğinin temin edilmesi,
— Kurum güveninin muhafaza edilmesi,
— Kurumsal itibarın korunması

için önem arz etmektedir. Bu çerçevede bir güvenlik riskinin gerçekleşmesini önleyebilmek ve gerçekleşmesi halinde en etkin şekilde müdahil olabilmek için çözümlerin sırasıyla

1. Caydırma
2. Algılama
3. Doğrulama
4. Geciktirme
5. Müdahale
6. Olay Sonrası İşlemler

Adımlarına yanıt verecek şekilde dikkatle ve sırası ile yerine getirilmesi gerekir. Şimdi bu adımların her birinde öne çıkan ve dikkat edilmesi gereken hususlara daha detaylı olarak bakalım.



1. Caydırma

> ***Güvenlik uygulamaları kapsamında "caydırma" herhangi bir güç kullanımı ya da müdahale faaliyetine gerek kalmaksızın kötü niyetli kişi ya da kişilerin faaliyetlerini yapmaktan vazgeçirilmeleridir.***

Alınan tedbirler ve yaratılan güvenli alan algısı ile potansiyel tehdit niteliğindeki kişi ya da kişiler herhangi bir riskin gerçekleşmesine neden olabilecek davranışlarından vazgeçirilmeye, caydırılmaya çalışılır. Alınan tedbirler ve oluşturulan güvenli alan algısı ile potansiyel tehditler, potansiyel davranışlarının bir sonucu olacağına, en iyisinin kötü niyetli bir davranışta bulunmamak olduğuna ikna edilmeye çalışılır. Fayda ve maliyet ekseninde değerlendirildiğinde en istenen sonuç henüz bir eyleme girişmeden kötü niyetli kişilerin faaliyetlerinden caydırılmasıdır. Bu kapsamda alınan her bir güvenlik tedbiri caydırma gayretinin bir parçasıdır. Hiçbir hırsız, güvenli tesis algısı kuvvetli olan bir tesise hırsızlık maksadıyla girmek iste-

mez. Bu kapsamda örnek vermek gerekirse;

- Tesis içerisinde açıkta malzeme bırakmamak,
- “Bu tesis 7/24 güvenlik kameraları ile izlenmektedir” tabelaları asmak,
- Güvenlik görevlileri ve/veya güvenlik araçları ile devriye faaliyet icra etmek,
- Güvenlik görevlisi istihdam etmek,
- Fiziki engel sistemleri,
- Güvenlik kameraları ve alarm sistemleri,
- Güvenlik faaliyetlerini talimat ve prosedürlere uygun yürütmek vb.

Tedbirlerin tamamı caydırıcı unsur niteliğindedir.

Henüz hiçbir güvenlik olayı yaşanmadan, kötü niyetli kişileri caydırmaya yönelik tedbirleri görünür kılmak, en etkili ve en düşük maliyetli uygulamadır.

Kurum bütçesinin en doğru şekilde yönetilebilmesi için caydırıcılık unsuru olan güvenlik çözümlerinin düşük maliyetliden daha maliyetli olana doğru hiyerarşik bir sıra ile kullanılması önem arz eder. Bu yaklaşım güvenlik risklerinin daha gerçekleşmeden bertaraf edilmesi için proaktif bir yaklaşım niteliğindedir.

2. Algılama

Caydırma gayretinin yetersiz kaldığı durumlarda tehdit niteliğindeki kişiler kötü niyetli faaliyetlerini uygulamaya girişiler.

Örneğin açıkta bulunan hurda malzeme alanında bakır kablo makaraları depolayan ve bu malzemeleri dışarıdan görülebilen, yeterli fiziki engel bulunmayan bir fabrikaya kötü niyetli kişilerin hırsızlık amacıyla girmek isteyecektir. Bu fabrikada hırsızlık riskinin gerçekleşme “olasılığı” ve gerçekleştiğinde

meydana gelecek “etkisi” yüksektir. Burada öncelikli olarak caydırıcı tedbirlerin alınması gerekir. Bu tedbirlere rağmen gerçekleşecek girişimleri tespit edebilecek algılama sistemleri de düşünülmelidir.

Caydırma gayretinin yetersiz kaldığı durumlarda potansiyel tehdit unsurlarını algılayacak güvenlik sistemleri tesis edilmeli, bu sistemlerin sürekli aktif ve etkin durumda olması sağlanmalıdır.

Örneğin bu vakada, ilk olarak açıkta bulunan malzemeler mümkünse kapalı alana alınmalı, fiziki engeller güçlendirilmeli, ikaz özellikli kameralar ya da alarm sistemleri ile algılama sistemi tesis edilmelidir.

Kimi zaman da bazı güvenlik zafiyetleri dış etkenlerin de etkisi ile güvenlik riskine dönüşür. Örneğin yanıcı maddelerin depolandığı depolarda sigara izmariti, cam ve güneş etkisi gibi sebeplerle yangınlar oluşabilir. İlk tedbir bu etki zincirini ortadan kaldırmak olmalıdır. Ancak meydana gelmesi ihtimaline karşı algılama sistemleri tesis edilmelidir. İşte bu algılama sistemleri de esasında bir yangın olayını engellemek için bir tür “caydırma” unsuru olarak da düşünülmelidir. Bu örnek durumda yangın algılama sistemi önemli ve gerekli bir tedbirdir. Bu tür durumların erken aşamada algılanabilmesi gerekli ve yeterli sistemlerin kurulmuş olmasına bağlıdır. Algılama etkin bir müdahalenin ilk adımıdır.

Zamanında algılanamayan her tehdit ve/ veya zafiyet bir riskin gerçekleşmesine sebep olacaktır.

Algılama sistemlerinin doğru ve etkin çalışması tehdit unsurlarının tespiti için ilk ve en önemli adımdır.

Örneğin bir tesis dış çevre hattında bulunan harekete duyarlı kameralar çok fazla yanlış alarm ürettiğinde bir süre sonunda hiçbir alarm kontrol edilmez hale gelecektir. Bu durum hiç alarm sistemi bulunmaması ile denktir. Algılanan bir ikazın güvenlik sistemi açısından bir tehdit olup olmadığının doğrulanması gerekir.

3. Doğrulama

Gerçekleşen bir olayın doğrulanması, olaya doğru yöntem ve esaslarla müdahale edilebilmesi açısından son derece önemlidir.

Doğrulama olayın ne olduğunun ve boyutunun anlaşılarak olaya uygun ekip ve doğru hareket tarzlarının belirlenmesi açsından son derece önemli bir faaliyettir.

Doğrulamanın gecikmesi ya da doğru yapılamaması durumunda olay hızla dramatik seviyede kötüleşebilir. Olayın anlaşılabilmesi için imkân dahilindeki tüm kaynaklardan doğrulama yapılmalıdır.

Örneğin bir dış çevre sınır hattındaki Harici Alarm Sisteminden (HAS) alarm geldiğinde varsa o bölgeyi gören kameralardan, olay bölgesinin yakınını gören kameralardan, o bölgede veya yakınında görev yapan güvenlik ekibinden duruma ilişkin bilgi alınmaya çalışılmalıdır. Bunların yanı sıra ayrıca yangın algılama sistemine düşen yangın ikazı, ikazın geldiği bölgeyi gören kameralar, bölgeye hâkim güvenlik noktaları aracılığı ile teyit edilerek detaylı bilgi alınmaya çalışılmalıdır.

Birden fazla kaynaktan yararlanılarak yapılan doğrulama, olayın en doğru şekilde anlaşılmasını sağlayacaktır. Böylelikle müdahale faaliyetlerinin olaya uygun olarak yapılabilmesi, aynı zamanda müdahale ekibinin can güvenliğinin sağlanmasını temin edecektir.

Müdahale için olayın türü ve boyutuna uygun, doğru ekibin yönlendirilmesi yapılmalıdır. Güvenlik yöneticileri ya da güvenlik kontrol merkezleri tarafından yapılacak yanlış bir yönlendirme,

olayın gelişiminin olumsuz yönde etkilenmesi, kurum itibarının zarar görmesi, mal veya can kaybı yaşanması veya artması gibi üzücü sonuçlara neden olabilir.

Örneğin, yangın ikaz sistemi üzerinden tespit edilen bir yangın ikazı o bölgeyi gören kameralar ile kontrol edilmeli, yakındaki güvenlik noktalarından teyit edilmeli ve bu yangın olayının bulunduğu yere tesis bünyesinde varsa öncelikle itfaiye personeli veya yangın eğitimi almış personel yönlendirmesi yapılmalıdır. Aksi halde yanlış müdahale, yangın tipine uygun olmayan müdahale ya da yangına müdahil olan kişilerin yangın ortamında doğru hareket tarzlarını bilmemeleri sonucunda yangının daha da büyümesi, ya da müdahale edenler dahil muhtemel can kayıplarının yaşanmasına neden olabilir. Doğrulamanın hemen ardından olay tipine ve boyutuna göre doğru ekibin yönlendirilmesi olası kayıpların en aza indirilebilmesi ve olayın süratle kontrol altına alınabilmesi için büyük önem taşır. Çoğu zaman istenmeyen bir faaliyetin doğrulanmasının ardından güvenlik ekibi müdahil oluncaya kadar geçecek bir süreye ihtiyaç vardır. Tam bu noktada güvenlik ihlali gerçekleştiren kötü niyetli kişi ya da kişilerin ekip müdahil oluncaya kadar geciktirilmesine ihtiyaç vardır.

4. Geciktirme

Riskleri ortadan kaldıracak ya da etkisini sınırlandıracak çözümler geliştirilirken ilgili "çözüm" risklerin doğrulanması ve ihtiyaç halinde müdahalesine imkân tanımalıdır. Başka bir deyişle,

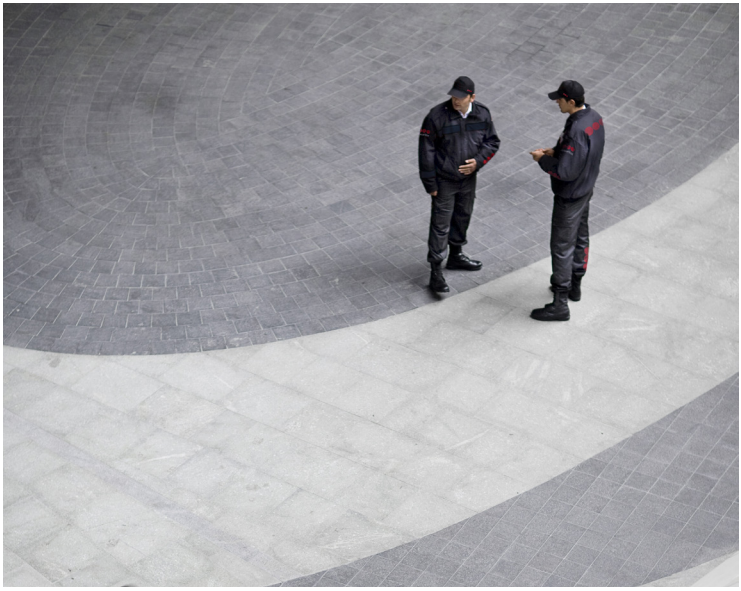
> ***Doğrulama aşamasının ardından müdahil oluncaya kadar geçecek sürede alınan çözümler güvenlik ekibinin fiziki müdahalesi için zaman kazandırabilecek nitelikte olmalıdır.***

Bir riski doğruladıktan sonra müdahil oluncaya kadar geçecek bir zamana ihtiyaç var. Güvenlik tedbirleri fiziki müdahale sağlanıncaya kadara geçecek sürede tehdit unsurunu geciktirecek nitelikte olmalıdır.

Çözümler güvenlik ekibinin fiziki müdahalesi için zaman kazandırabilecek nitelikte olmalıdır. Çünkü doğrulama aşamasından müdahale ekiplerinin olaya müdahil olmasına kadar geçecek bir süreye ihtiyaç vardır. Tam bu noktada, alınan tedbirlerin müdahale gerçekleşinceye kadar mevcut durumun daha da kötüye gitmesini engelleyebilecek nitelikte olması gerekir. Bu doğrulama ile müdahale arasında geçecek sürenin risk türüne uygun tedbirlerle takviye edilmesi anlamına gelir. Çünkü riskin çeşitli vasıtalarla ilk doğrulandığı andan, ilk müdahale ekibinin bu riske müdahil olacağı ana kadar geçecek bir süre söz konusudur. Bu süre zarfında müdahale ekibinin olaya müdahalesine kadar riskin dramatik seviyeye ulaşmasını engelleyecek yavaşlatıcı veya durdurucu nitelikte ilave tedbirler olmalıdır. Potansiyel olarak tanımlanan bir riskin gerçekleşmesi bazı senaryolarla mümkün olur. Geliştirilen çözüm öngörülen senaryolar gerçekleştiğinde, ilgili konunun doğrulanması ve müdahalesine imkân tanımalıdır.

Örneğin, “Mülke İzinsiz Giriş” riski birçok senaryo ile gerçekleşebilir. Bu örneğimizde bu riskin “Acil Çıkış Kapısından Kontrolsüz Olarak Girme” senaryosu ile gerçekleşeceğini var sayalım. Bu riski engellemek için geliştirilen çözüm hem doğrulama hem de müdahaleye imkân tanımalıdır. Örnek olarak bu risk ve senaryo için geliştirilen çözümün alarm ikazı bulunan bir yazılımlı kamera ve kameraya entegre hoparlör olduğunu varsayalım. Bu senaryo gerçekleşip, şüpheli bir kişinin acil çıkış kapsını zorla açıp binaya kontrolsüz olarak girmesi halinde yazılımlı kamera ikaz verecek ve gerçekleşme aşamasında olan riskin uzak izleme merkezi ya da kurum içindeki izleme merkezince (CCTV merkezi) doğrulanması sağlanacaktır. Acil çıkış kapısından kontrolsüz olarak giriş tespit edilip, böyle bir olayın gerçekleştiği doğrulandıktan sonraki işlem ise müdahaledir. Buradaki müdahale devriye ekibinin olay bölgesine gönderilmesi veya kameraya entegre edilmiş hoparlör ile gerçekleştirilebilir. Ancak devriyenin buraya

ulaşması için bir zamana ihtiyaç olduğundan, ilk müdahalenin hoparlörden anons yapılarak gerçekleştirilmesi devriye ekibi buraya ulaşıncaya kadar zaman kazandıracaktır. Kontrolsüz olarak giriş yapan kişinin eylemi tespit edilip, kaçak giriş olduğu doğrulanıp, hoparlör ile müdahale edildiğinde genellikle bu kaçak giriş engellenecek ya da kaçak giriş yapmaya çalışan kişi tereddüt yaşayacaktır. Bu çözüm devriye ekipleri olay yerine ulaşıncaya kadar zaman kazandırabilecek bir çözümdür. Ya da bir yangın olayının tespit edilip doğrulanmasının ardından yangını söndürme ekibi ya da itfaiye ekipleri müdahil oluncaya kadar geçecek bir süreye ihtiyaç vardır. Yangın ilk birkaç dakikada çok hızlı ilerleme kaydeden bir felakettir. Ekipler yangına müdahil oluncaya kadara geçecek sürede yangının etkisinin geciktirilmesine ihtiyaç vardır. FM200 sistemin devreye alınması, söndürme sistemlerinin aktif edilmesi gibi ilk müdahale işlemleri yangının yüksek etkiye ulaşmasını geciktirebilir hatta tamamen engelleyebilir. Bu da müdahale ekiplerine büyük kolaylık sağlayacaktır.



5. Müdahale

Meydana gelen olaylar tesise, tesiste bulunan tüm paydaşlara ya da marka değerine ve kurumsal itibara zarar verebilir. Olaya müdahale faaliyetlerinin özünde; olayın gerçekleştiği andan itibaren olayın olası tüm etkilerini en aza indirmek, tesis ve paydaşlara etkisini bir an önce sınırlandırmak için olabildiğince hızlı cevap verme ve olabildiğince hızlı şekilde toparlanma gayreti vardır. Zamanında ve doğru şekilde müdahale edilemeyen küçük bir olay dahi büyüyerek önemli zararlara neden olabilir. Etkin ve doğru bir müdahale için en önemli faktörlerden biri müdahale anı faaliyetleri kadar, müdahale anından önce, o ana kadar yapılan hazırlıkların seviyesidir.

Müdahale öncesi hazırlık dönemi ihtiyaç duyulan eğitim ve tatbikatlarla ne kadar doğru ve etkin yönetilirse, müdahale de o seviyede doğru bir zeminde gerçekleşecektir.

İyi bir hazırlık döneminin çıktısı olaylara müdahale planıdır. Hazırlık döneminde;

- Uygun prosedür ve talimatların geliştirilmesi,
- Muhtemel güvenlik olayları ve her olaya özgü müdahale yöntemlerinin belirlenmesi
- Acil durum iletişim hiyerarşisinin belirlenmesi
- Acil durum türüne göre müdahale ekiplerinin belirlenmesi
- Tetikleme mekanizmalarının belirlenmesi
- Eğitim ve tatbikatlarla istenen hareket tarzlarının pekiştirilmesi

gibi faaliyetler olay anında müdahalenin en doğru şekilde gerçekleştirilmesini sağlayacaktır. Ayrıca olay öncesinde muhtemel olaylar ve olası etkilerini ortaya çıkaran bir risk analizi yapılması, olayların etkileri ve öncelikleri göz önünde bulundurularak uygun çözümlerin geliştirilmesi önem arz eder.

6. Olay Sonrası İşlemler

Yaşanan bir acil durumun ardından işyeri / tesisin süratle ana faaliyet düzenine dönmesi gerekmektedir. Öte yandan acil durum sonrasında adli, idari ve kurumsal gereklilikler ve sigorta kapsamında ihtiyaç duyulacak kayıt, evrak, tutanak vb. tam olarak tanzim edilmeli, ayrıca tesis tam olarak hazır olduktan sonra üretim ya da hizmete devam etmelidir. Unutulmamalıdır ki hizmetin ya da üretimin; fiziksel açıdan, ekipman ve personel açısından tam olarak hazır hale gelmeden başlatılması atlatılan acil durumun gerçekte olduğundan daha fazla zarar verdiği algısına neden olacaktır. Bu nedenle hizmet / üretim başlamadan önce kurumun Acil Durum Planlarında bulunan faaliyete başlama kontrol çizelgesine göre kontroller sağlanarak faaliyete başlanmalıdır. Acil durum sonrasında;

- Olaya ilişkin itfaiye, polis / jandarma veya diğer kamu görevlileri tarafından düzenlenen tutanak, olay inceleme raporu, olay raporu gibi dokümanların bir kopyası temin edilmelidir.
- Olay anı kamera görüntüleri arşivlenmelidir.
- Olay anına ilişkin delil niteliğindeki malzeme korunmalıdır.
- Olay türü ve boyutuna bağlı olarak, gerekmesi halinde olay mahalli muhafaza edilmelidir.

Securitas Güvenlik Metodolojisi
Dördüncü Adım:

Uygulama

Uygulama

Kurum ile anlaşmaya varılması ve sözleşme imzalanması durumunda üzerinde anlaşmaya varılan güvenlik çözümlerinin zamanında, tam olarak ve aksamadan başlatılması ve sürekli olarak sistem testleri ile gelişim alanlarının araştırılması uygulama adımını oluşturur.

Uygulama aşaması kendi içerisinde iki safhada yürütülür.

— Birinci safha, hazırlıkların başlatılması ve tamamlanması,
— İkinci safha ise hizmeti yürütmedir.

Kurum ile sözleşme imzalandıktan sonra sözleşmede taahhüt edilen tarihe kadar gerekli hazırlıklar yapılır ve güvenlik hizmeti başlatılır. Bu sürecin en doğru ve eksiksiz şekilde yürütülebilmesi için tüm başlatma faaliyetlerini kapsayan Securitas Hizmet Başlatma Prosedüründen bu aşamada istifade edilmektedir.

Hizmet başlatma süreci, güvenlik hizmetinin başlatıldığı tesis / iş yeri için hassasiyetin en yüksek olduğu dönemdir. Bu dönemde güvenlik riskleri ile karşı karşıya kalınmaması için bu sürecin bir plana göre yürütülmesi önem arz eder.

Bir plan ve kontrol listelerine bağlı olarak başlatılan güvenlik hizmetinde olası aksaklıklar en aza inecektir. Hizmetin başlatıl-

masının ardından hizmet yürütme sürecinde en önemli husus taahhüt edilen tüm hizmetlerde devamlılığın sağlanması ve Kurum'a değer yaratılmasına devam edilmesidir. Kurum için değer yaratılmaya devam edildiği sürece sürdürülebilir bir iş ilişkisi sağlanabilir. Bu kapsamda, mevcut hizmetin Kurum ihtiyaçları, güncel gereklilikler ve gelişmeler doğrultusunda geliştirilmesi ve/veya dönüştürülmesi değerlendirilmelidir. Bu yolla hizmet etkinliği sürekli arttırılarak güvenlik maliyetleri kapsamında Kurum lehine avantaj sağlanabilir.

Etkili ve maliyet avantajı yaratan bir hizmet, Securitas ve hizmet verdiği Kurum için "değer" üreten bir hizmet olacaktır.

Değer üretebilmenin bir başka yolu, güvenlik hizmetinin ölçülebilir, izlenebilir ve raporlanabilir yanlarının güçlendirilmesidir. Bu maksatla, mümkün olan her halde süreçlerin dijital platformlara aktarılması önem arz eder. Bu bakış açısı kurumun verimliliğini artırırken Securitas açısından sürdürülebilir bir hizmete imkân tanır.

Securitas Güvenlik Metodolojisi kapsamında hizmet yürütme prensiplerinin dikkatle uygulanması, esasları önceden belirlenmiş yöntemlerle kontrol edilmesi sürdürülebilirliğin sağlanmasına katkı sağlayacaktır.


Securita
Securitas

Securitas Güvenlik Metodolojisi
Beşinci Adım:

Kalite Kontrol

Kalite Kontrol

Kalite kontrol, ürün veya hizmetlerin belirlenen standartlara ve gerekliliklere uygunluğunu denetlemek amacıyla gerçekleştirilen doğrulama faaliyetleri ile bu faaliyetler sırasında kullanılan yöntem ve araçların bütünüdür.

> ***Ürün ve hizmet üretiminde Kurumların ihtiyaç, istek ve beklentilerini göz önünde bulundurmayan işletmeler, Kurumların beklentilerini karşılayan işletmeler karşısında pazar paylarını kaybetmeye mahkûmdur.***

Kalite Kontrol; belirli bir takvime bağlı kalınarak, yürütülmekte olan güvenlik hizmetinin;

- İlgili kanun ve mevzuata uygun olarak yürütülüp yürütülmediğinin kontrolünün
- Securitas prosedür ve talimatlarına göre uygunluğunun
- Kurum ihtiyaçları ve beklentileri ile uyumunun

devamlı olarak gözden geçirilmesi, tespit edilen aksaklıkların iyileştirilmesi ve sonuçların raporlanmasıdır. Hizmet kalitesinin devamlılığının sağlanabilmesi için sunulan hizmetin sözleşme gereklerini karşılayıp karşılamadığı ve/veya operasyonel süreçlerde aksayan hususların olup olmadığı çeşitli kalite kontrol uygulamaları ile kontrol edilir. Bu kapsamda yapılan işlemlerin tümü kalite kontrol faaliyetleridir.

Rekabet gücünü elde etmenin temel şartlarından biri de Kurumlerin ihtiyaç, istek ve beklentilerine uygun olarak kaliteli bir hizmet sağlamaktır.

Kalite kontrol uygulamalarının altında yatan temel yaklaşım;

— Kontrol et,
— Aksaklığı tespit et,
— İkaz et,
— Aksaklığı gider,
— Ders al,
— Eğit,
— Durumu iyileştir,
— Sürdür prensiplerini izlemektir.

Bu amaçları gerçekleştirmek ve kaliteli hizmet sunumunun devamlılığını sağlamak için çeşitli uygulamalar yapılır. Kalite kontrol uygulamaları, Kurum memnuniyeti kapsamında güvenlik hizmetinin kalitesinin ölçülmesinin en önemli göstergelerinden biridir.

Güvenlik Hizmetinin "Kalite Kontrol"ü aşağıda belirtilen faaliyetlerle yerine getirilir.

a. Yerinde Denetlemeler

Securitas bünyesinde Bölge Müdürlükleri tarafından oluşturulan ***Bölge Aylık Denetleme Planına*** uygun olarak denetlemeler; şube müdürleri, bölge denetleme şefleri, kontrol hizmetleri personeli, Kalite Departmanı Eğitim ve Denetim Uzmanları ve uzaktan izleme merkezi operatörleri tarafından aşağıdaki esaslara göre yerine getirilir:

1. Denetleme öncesinde denetlenecek birimin bir önceki denetlemede tespit edilen eksiklikleri Denetleme Eksiklik Raporundan incelenir.
2. Securitas'ın güvenlik hizmetinin yönetmesine yardımcı olan Smart yazılımında bulunan denetleme gruplarından yapılacak denetlemeyle ilgili grup seçilir.
3. Denetlemesi yapılacak konuların seçiminde öncelikle önceki denetlemelerde eksik olarak tespit edilen hususlar ile düşük puan almış soru gruplarına öncelik verilir.

4. Kurum ile paylaşılmış olan risk bildirimlerinin mevcut durumu incelenerek devam eden riskler için yeni bildirim hazırlanır.
5. Denetlenecek olan grup ya da soru/sorular, öncelikle geçmişe ait denetleme sonuçlarına göre belirlenir.
6. Soruların değerlendirilmesinde objektif ölçütler esas alınmalıdır.
7. Evet/hayırlı değerlendirmede "hayır" seçeneği, çoktan seçmeli soruların değerlendirmesinde ise "orta", "kötü" ve "çok kötü" seçenekleri seçildiğinde; açıklamalar bölümüne seçimin gerekçesi ve alınması gereken önlemler konusunda açıklama yazılır.
8. Denetlemede tespit edilen iyileştirme alanlarının eşzamanlı olarak görev başı eğitimlerle giderilmesine öncelik verilir.
9. Bir birimde genel denetleme ve kişisel denetleme uygulanma oranının birbirine yakın olması beklenir.
10. Şube müdürleri Smart kayıtlarında denetleme eksiklik rapor bölümünü inceleyerek daha önce yapılan denetlemelerde tespit edilen eksikliklerin tamamlanması için gerekli çalışmaları yapar.

b. Drill (Farkındalık Testi) Uygulamaları

Drill (farkındalık testi), Kuruma verilen güvenlik hizmetlerinin bir senaryoya bağlı kalınarak denetlenmesidir.

Örneğin; bir AVM'de verilen kapı güvenliği hizmetinde şüpheli çanta ve paketlere karşı alınması gereken önlemlerin ne doğrulukla yapıldığı bir senaryoya bağlı kalınarak test edilir. Drill faaliyeti aşağıdaki esaslar çerçevesinde gerçekleştirilir.

1. Bu tür denetlemelerde denetlenen personelin senaryodan haberi olmaz ve denetleyici denetleme yapıldığını belli etmez. Uygulamalara ilişkin değerlendirmeler, mümkün olduğunca kamera kayıtları izlenerek yapılır.
2. Yapılacak tüm drill faaliyetleri (senaryo konusu, zamanı, yeri vb.) önceden Kurum Temsilcisine/Güvenlik Müdürüne ve ilgili Bölge Müdürlüğü'ne yazılı olarak bildirilir.
3. Drill'in uygulamasından bir ya da iki gün önce Kurum Temsilcisi/Güvenlik Müdürü ile konu detaylı bir şekilde görüşülür ve gerekiyor ise Kurumun diğer departmanları bilgilendirilir. Bu kapsamda, olası yanlış anlaşılmalardan kaynaklanabilecek panik vb. durumların oluşmasına engel olunur.
4. Drill Şube Müdürlüğü tarafından yapılıyorsa sahte eşyaların ilgili yere sokulması, drill'e hazır hale getirilmesi Şube Müdürü kontrolünde, Şube Şefi ya da Kurum Temsilcisi/Güvenlik Müdürü tarafından uygun görülen yöntemler ile gerçekleştirilir.
5. Drill'in başlangıcından itibaren, sürecin kameralar ile mi yoksa bizzat mı izleneceği, bizzat izlenecekse kim tarafından, nerede, nasıl izleneceği belirlenerek ilerlenir.
6. Drill'e tabi tutulan personelin nokta özel talimatında belirtilen hususları ne doğrulukla yerine getirdiği nokta özel talimatı esas alınarak hazırlanacak olan bir kontrol formu üzerinden değerlendirilir. Örneğin, nokta özel talimatında "Metal el detektörü ile ziyaretçinin bacakları, kolları ve gövdesi taranır." gibi bir ifade varsa "Metal el detektörü ile ziyaretçinin bacakları, kolları ve gövdesi tarandı mı?" gibi bir kontrol sorusu oluşturulabilir.
7. Drill uygulaması sonucunda yapılan değerlendirmeler Securitas'ın güvenlik hizmetinin yönetmesine yardımcı olan Smart web uygullaması üzerindeki ilgili değerlendirme formuna girilir.
8. Operasyonel ve zorunlu ihtiyaçlar dışında başarılı veya


Securitas

başarısız bir drill uygulamasından sonra aynı birimde uygulanacak bir drill için asgari üç aylık sürenin geçmesi ve bu sürenin bir önceki drill sonucuna göre düzeltici ve/veya geliştirici faaliyetlerin yerine getirildiği bir zaman olarak değerlendirilmesi gerekmektedir.

9. Drill çalışmasından sonra mutlaka ilgili birimde görevli ve drill uygulanan personel, Kurum yetkilisi (mümkünse), birimde bulunan Securitas Saha Yöneticileri ve şube müdürlüğünün katılımı ile faaliyet sonu incelemesi yapılır. Bu incelemede ne yapıldı, ne yapılmalıydı, nasıl daha iyi olurdu? Sorularına yanıt aranır. Bu inceleme sonucuna göre, gerekiyorsa görev yeri talimatları ve uygulama esaslarında değişiklik yapılır. Değerlendirme neticesinde ihtiyaç görülürse eğitim planlaması yapılır.

c. Uzaktan Denetim Hizmeti

Uzaktan denetim hizmeti, Securitas Uzaktan İzleme Merkezi (UİM) ile sesli iletişime imkân tanıyan bir kamera ve ek tertibatından oluşan sistem üzerinden yapılır. Bu denetimlerde amaç, projelerde/birimlerde görev yapan güvenlik görevlilerinin görevlerini nokta özel talimatında belirtildiği şekilde yapıp yapmadığının yetkili personel tarafından kontrol edilmesidir.

1. Güvenlik Görevlilerinin görev yaptığı noktalara (GKM, nizamiye, kapı, kontrol noktası vb.) kurulan uzaktan denetim kameraları uzaktan izleme merkeziyle iletişimini sim kart üzerinden sağlamaktadır.
2. Uzaktan denetimler Kuruma özgü standardize edilmiş bir kontrol formuna göre UİM operatörleri tarafından yapılır.
3. Denetim sonuçları ilgili Şube Müdürlüğüne ve Kalite Departmanı'na sistem tarafından otomatik olarak e-posta ile gönderilir.

Gerçekleştirilecek denetimlere güncel teknolojik imkânların dahil edilmesi hem gelişim alanlarının tespitine hem de operasyonel birimlerin farkındalığının artmasına katkı sağlayacaktır. Uzak Denetim Kameraları bu araçlardan biridir.

4. Şube Müdürleri ile yetki verilen Kalite Departmanı ve MGM personeli kendilerine UİM tarafından açılan immix hesapları üzerinden kamera görüntülerine ve uzaktan izleme merkezinin yaptığı denetimlerin görüntü ve sonuçlarına ulaşabilirler.

d. Kalite Departmanı Denetimleri

Kalite Departmanı denetimleri, bir kalite kontrol aracı olarak Kalite Departmanı tarafından planlanan ve icra edilen denetim faaliyetleridir. Planlama, Kalite Departmanı tarafından; proje ihtiyaçları, güncel güvenlik riskleri ve Kurum beklentileri göz önünde bulundurularak yapılır. Kalite Departmanı çalışanları tarafından icra edilen denetim faaliyetleri öncesinde ilgili şube müdürlüklerine bilgilendirme yapılır. Bu bilgilendirme doğrultusunda varsa projeye ilişkin hassasiyetler Kalite Departmanı'na bildirilir. (Denetimde dikkat edilecek özel hususlar, Kurum hassasiyetleri, sözleşme hassasiyetleri, güvenlik riskleri vb.) Bu koordinasyon çerçevesinde denetim icra edilir.

e. KPI (Anahtar Performans Göstergeleri) Takibi

Anahtar performans kriterleri, ölçümlemesi yapılacak olan hususları ifade etmektedir.

1. Şube Müdürlükleri esasları Kalite Departmanı tarafından belirlenen KPI esasları çerçevesinde bir KPI sistemine dahildir.
2. Bu denetimler Smart KPI Modülünden otomatik olarak yapılır.
3. Şube Müdürleri Kalite Departmanı Şube KPI Denetleme Prosedürü'nde yer alan anahtar performans kriterleri esas alınarak yüz puan üzerinden not verilerek değerlendirilir. Bu değerlendirme sonuçları Bölge ve Şube bazlı periyodik olarak yayınlanır ve Smart[6] üzerinden takip edilebilir.

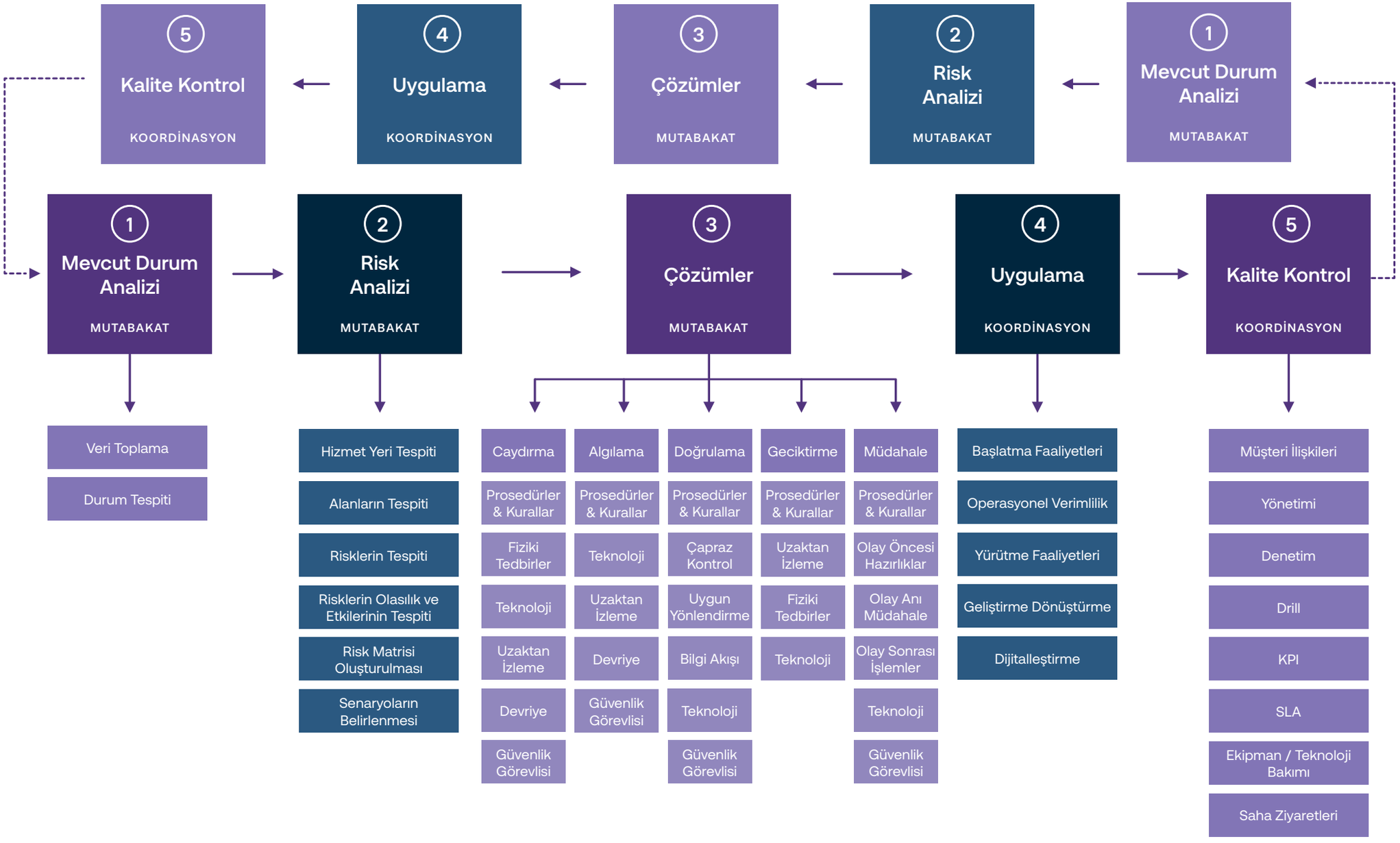
---

[6] *Smart: Securitas bünyesinde kullanılan özel bir yazılımdır.*

Securitas Güvenlik Metodolojisi İş Akışı

Securitas Güvenlik Metodolojisi, güvenlik hizmeti alan işletmelere, bu alana yönelik beklentilerinin üzerinde çözümler sunmaktadır. Bir bütünlük içerisinde, sürdürülebilir güvenlik hizmetinin taklit edilemez olması ise güvenlik alanında Securitas'ı farklı kılan ve sektör lideri yapan önemli unsurlardan birisidir.

Securitas Güvenlik Metodolojisi İş Akışı



Kaynakça

— ALTUN, Bilal. 2017. «Kurumsal Stres Kaynakları ve Stresle Başa Çıkma: Beylikdüzü Belediyesinde Bir Uygulama (Yüksek Lisans Tezi).» Göller Bölgesi Aylık Hakemli Ekonomi ve Kültür Dergisi Ayrıntı Sayı 49 58-65.
— ARPAT, Recep Sait. 2016. Acil Durum ve Kriz Yönetimi. Gece Kitaplığı.
— COŞKUN, Seyit. Haziran 2018. «Sosyal Bilimlerde Metodloji Problemi.» Dört Öge 13, 59-72.
— ÇALIŞKAN, Feramuz. 2021. «Güvenlik Uygulamaları Kapsamında “Risk İştahı” Kavramı.» Linkedin. 21 Eylül. https://www.linkedin.com/in/feramuzcaliskan/.
— ÇEVİK, Prof Dr Hasan Hüseyin. 2013. «Özel Güvenlik Hizmetlerinde Verimlilik ve Etkililik İlkeleri.» Özel Güvenlik Hizmetlerinde GÜvenlik Önlemleri içinde, yazan Editör Prof Dr Hasan Hüseyin ÇEVİK, 2-19. Eskişehir: Anadolu Üniversitesi.
— Doç Dr Ruziye COP, Ayşe YÜZÜAK. 2016. «Değer Temelli Pazarlamada Müşteri Değerine, Firma ve Müşteri Bakış Açısından Bolu İlinde Bir Uygulama.» Gazi Üniversitesi İktisadi ve İdari Bİlimler Fakültesi Dergisi 49-80.
— Doç. Dr. Melike TEKİNDAL, Araş. Gör. Şerife UĞUZ ARSU. 2020. «Nitel Araştırma Yöntemi Olarak Fenomenolojik Yaklaşımın Kapsamı ve Sürecine Yönelik Bir Derleme.» Ufkun Ötesi Bilim Dergisi 153-182.
— GÖRMEN, Murat. 2018. «ÖRGÜT KÜLTÜRÜ İLE RİSK KÜLTÜRÜ ARASINDAKİ İLİŞKİNİN İNCELENMESİ.» Balkan Sosyal Bilimler Dergisi 121-135.
— HOPKIN, Paul. 2017. Fundamentals of Risk Management, Understanding, Evalluating and Implementing Effective Risk Management. Newyork: Kogan Page Ltd.
— International, ASIS. 2005. Business Continuity Guideline, A Practical Approach for Emergency Preparedness, Crisis Management and Disaster Recovery. ASIS International.
— İŞTAR, Araş Gör. Emel. 2012. «Stres ve Verimlilik İlişkisi.» Akademik Bakış Dergisi.
— KANAT, Emine Büşra. 2020. Metodoloji Nedir? 20 Ocak. https://www.iienstitu.com/blog/metodoloji-nedir.
— LAM, James. 2015. Implementing an Effective Risk Appetite. Montvale, NJ: The Association of Accountants and Financial Professionals in Business.
— ÖZALP, Hakan. 2016. Özel Güvenlik Risk Yönetim Sistemi. İzmir.
— ÖZER, Yrd Doç Dr Uğur. tarih yok. «Toplam Kalite Yönetimi.»
— Prof Dr Handan TÜRKOĞLU, Yrd Doç Dr Reyhan YİĞİTER. 2001. Acil Durum Planlaması. İstanbul: İTÜ Afet Yönetim Merkezi.
— Prof. Dr. Deniz TAŞÇI, Yrd. Doç. Dr. Sayen Nihan ÇABUK. 2013. Kalite Yönetim Sistemleri. Eskişehir: Anadolu Üniversitesi.
— SINEK, Simon. 2020. Neden İle Başla. İstanbul: Arıtan.
— TOKER, Kerem. 2018. «Endüstri 4.0 ve Sürdürülebilirliğe Etkileri.» İstanbul Management Journal 51-64.
— ÜNVER, Oryan. tarih yok. Risk ve Risk Değerlendirmesi. İstanbul: GÜSOD.
— tarih yok. Wikipedia Metodoloji Nedir? https://tr.wikipedia.org/wiki/Metodoloji .
— WINBERG, Hakan. 2019. Yaklaşık Olarak Doğru. Ankara: Bilgi Yayınevi.
— Yrd. Doç DrFerit KÜÇÜK, Yrd. Doç. Dr M. Nedim BAYUK. Aralık 2007. «Kurum İçi Stres Kaynaklarının Kurumsal Bağlılığa Etkisi: Şanlıurfa Belediye Örneği.» Çağ Üniversitesi Sosyal Bilimler Dergisi 66-89.

GÜVENLİK ÇÖZÜMLERİ METODOLOJİSİ

Güvenlik süreçleri bir metot içermediğinde gözden kaçan risklerin oluşturacağı zararlar önlenemez. Bu nedenle SGM aslında ISO 31000 ışığı altında risk temelli çözüm üretip ölçülebilirliği ve sürdürülebilirliği ön plana çıkaran iş yapış şeklimizdir.

Berti Bora
Securitas Risk Yönetimi ve Danışmanlık Hizmetleri Genel Müdürü

Her bir işletmenin temel hedeflerinden biri olan sürdürülebilir olma; işletmelerin rutin faaliyetlerini yerine getirirken risk teşkil edebilecek her bir tehdidi önceden görerek olası hasarlarını en aza indirmelerine imkân verecek tedbirleri almalarıyla mümkündür.

Securitas Güvenlik Metodolojisi; bu kapsamda yapılacak çalışmalarda izlenecek yol ve yöntemleri ihtiyaç sahiplerine aktarmak maksadıyla hazırlanmış, güvenlik sektörü için son derece faydalı bir dokümandır.

Hüseyin Erim
Güvenlik Süreçleri ve Kalite Koordinatörü

Güvenlik operasyonun temelini teşkil eden risk yönetiminin uçtan uca nasıl ele alınması gerektiğini anlatan; ideal güvenlik kurgusunun oluşturulmasından, hizmetin belirli kalite standartlarında sürdürülebilir bir şekilde yürütülmesine kadar uygulanması gereken adımları oldukça detaylı bir şekilde tarifleyen harika bir kılavuz. Emeği geçen herkese çok teşekkürler.

Gökhan Usta
Güvenlik Süreçleri Kalite Müdürü

Securitas