COĞRAFİ BİLGİ SİSTEMLERİ GENEL MÜDÜRLÜĞÜ

Akıllı Şehir Rehberlik Uygulamaları Projesi

AKILLI ŞEHİR SİBER GÜVENLİK SİSTEMLERİ

T.C. Çevre, Şehircilik ve İklim Değişikliği Bakanlığı © 2024

AKILLI ŞEHİR SİBER GÜVENLİK SİSTEMLERİ REHBERLİK KILAVUZU

Bu kılavuz, akıllı şehir uygulamalarından olan "Siber Güvenlik Sistemleri" oluşturmak isteyen kurum ve kuruluşlara, projenin geliştirme ve uygulama aşamalarında destekleyici rehber doküman olması amacıyla hazırlanmıştır.

Kılavuzda uygulamaya yönelik bir vaka üzerinden aşamalı ve detaylı olarak açıklama yapılmıştır.

Rehberlik kılavuzu ile uygulamanın projelendirilmesine ve fizibilite çalışmalarının yapılmasına destek olunması hedeflenmektedir.

1. Projenin Tanımı

"Akıllı Şehir Siber Güvenlik Sistemleri" projesi ile akıllı şehir uygulamaları için kullanılan tüm Nesnelerin İnterneti (IoT) cihazlarının ve dijital sistem verilerinin tek bir merkezde toplanarak; takibinin, güncellenmesinin, yönetiminin ve güvenliğinin sağlanması amaçlanmaktadır.

1.1. Projenin Adı, Uygulama Yeri ve Süresinin Belirlenmesi

- Projenin adı belirlenir.
- Siber Operasyon Merkezi (SOM) ve IoT Güvenli Haberleşme Modülü gereksinimleri tanımlanır.
- Projenin uygulama alanı, büyüklüğü ve yapısı belirlenir.
- Proje süresi belirlenir.
- Akıllı Şehir Proje Yönetimi Standartları kapsamındaki Proje Fişleri hazırlanır.

Örnek Vaka	
Proje Adı	Akıllı Şehir Siber Güvenlik Sistemleri Projesi
Uygulama Alanı	1000 Ha yerleşim alanı – 200.000 kişi
Proje Süresi	Proje süresi 14 ay aydır.
Akıllı Şehir Proje Fişi, Akıllı Şehir Proje Yönetimi Standartları kapsamında hazırlanmış olup dokuman www.akillisehirler.gov.tr adresinde yayınlanan Akıllı Şehir Bilgi Paylaşım Portalı'ndan erişilebilmektedir.	

1.2. Proje Teknik Bileşenleri

Akıllı Şehirlerde Siber Güvenlik Sistemleri projesi için gerekli olan teknik bileşenler öncelikle genel olarak sıralanmakta, ardından bölümün devamında gerekli görülen teknik bileşenler açıklanmaktadır:

- Siber Operasyon Merkezi (SOM)
- IoT Güvenli Haberleşme Modülü
- Ağ Güvenliği
- Veri Güvenliği
- Fiziksel Güvenlik
- Sistem ve Uygulama Güvenliği
- Güvenlik Olayı Yönetimi (SIEM)
- Endüstriyel Kontrol Sistemleri Güvenliği (ICS)
- Mobil ve Kablosuz Güvenlik
- Güvenlik Politikaları ve Farkındalık
- Acil Durum Müdahale ve Kurtarma Planları
- Yedekleme ve Kurtarma (Backup & Recovery)
- Büyük Veri ve Veri Analitiği Güvenliği
- Blockzincir Teknolojisi

Siber Operasyon Merkezi (SOM): Bir organizasyonun güvenliğini izleyen ve güvenlik olaylarının analizinden sorumlu bir bilgi güvenliği ekibinin bulunduğu yerdir. Teknolojik çözümler kullanarak güvenlik olaylarını tespit eder ve analizini yapar, aksiyon alarak siber saldırılara karşı önlem alır.

IDS (Intrusion Detection Systems): Ağ trafiğindeki zararlı hareketleri veya bağlantıları tespit etmek ve loglamak için kullanılan sistemdir. Temel amacı saldırıları algılamak ve kayıt altına almaktır.

IPS (Intrusion Prevention Systems): Ağ trafiğindeki zararlı hareketleri veya bağlantıları tespit ederek önlem almak için kullanılan güvenlik sistemidir. Saldırıları algılar ve engeller, böylece zararlı etkileri önler.

DLP (Data Loss/Leak Prevention): Veri kaybı ve sızıntısını önlemek amacıyla kullanılan bir veri koruma sistemidir. DLP yazılımları ile istenmeyen verinin çıkışı engellenebilir ve belirli dosyaların kullanım durumları izlenebilir.

ENDPOINT SECURITY: İstemci cihazları ve diğer kablosuz cihazları koruyarak uzaktan köprülenmiş bilgisayar ağlarını savunmaya yönelik bir yaklaşımdır. Gelişmiş bir savunma sağlayarak yeni nesil antivirüs, tehdit algılama, cihaz yönetimi ve veri sızıntısı koruması gibi özellikleri içerir.

SIEM (Security Information Event Management): Logları toplayarak anlamlandıran ve alarm üreten merkezi bir loglama ve yönetim bileşenidir. Farklı kaynaklarda bulunan cihazlardan oluşan anormallikleri tespit ederek NOC ve SOM ekiplerine alarm üretir ve alınacak önlemleri belirler.

SOAR (Güvenlik Düzenleme Otomasyon ve Yanıt): Güvenlik tehditlerini izlemeye ve küçük olaylara insan müdahalesi olmadan yanıt vermeye olanak tanır. Bu sayede veri çeşitliliğinin artması karşısında tehdit müdahale yetenekleri geliştirilir ve iş süreçleri kolaylaşır.

GRC Sistemleri: Kurumsal riskleri sistemli bir şekilde yönetmeye yardımcı olur ve saldırılara erken müdahale sağlar.

UTM (Unified Threat Management): Güvenlik duvarı, antivirüs, antispam, IDS/IPS, VPN ve router gibi özellikleri bir araya getiren tümleşik cihazlardır. Tehditlere karşı kapsamlı koruma sağlar ve web filtrelemesi ile dosya indirme gibi işlemleri kontrol altına alır.

NGFW (Yeni Nesil Güvenlik Duvarı): Geleneksel güvenlik duvarlarının diğer ağ cihazı filtreleme işlevleriyle birleştirilerek üçüncü nesil güvenlik duvarı teknolojisi oluşturulmasını sağlar.

Siber Güvenlik Merkezi Ekibi (SOME): Uygun yetkinliklere sahip personellerin oluşturduğu bir ekiptir ve güvenlik operasyonlarını yönetmekle görevlidir.

IoT Güvenli Haberleşme Modülü: Güvensiz haberleşme protokollerini güvenli hale getirerek IoT cihazlarından gelen verilerin filtrelenmesini ve şifrelenmesini sağlayan bir sistemdir. Verilerin sadece alıcının deşifreleyebileceği şekilde korunmasını amaçlar.

1.3. Proje Girdileri

Akıllı Şehir Siber Güvenlik Sistemleri için proje girdileri şunlardır:

- Uçtan uca güvenlik kapsamında IoT cihazlarından gidecek şifreli verileri gönderen verici modül
- Uçtan uca güvenlik kapsamında IoT cihazlarından gelen şifreli verileri alan alıcı modül
- Verilerin taranması ve güvenli şekilde izlenebilmesi, toplanması ve depolanması amaçlı SOM
- SOM'da kullanılacak uygulamalar (Güvenlik Duvarı, SIEM, vb.)
- SOM'da kullanılacak donanımlar (Ağ güvenlik cihazları, router, vb.)

1.4. Beklenen Çıktılar

Akıllı Şehir Siber Güvenlik Sistemleri kapsamında beklenen çıktılar aşağıdaki gibidir:

- Akıllı şehir uygulamaları için kullanılan IoT cihazlarının veri güvenliğini sağlamak.
- Siber güvenlik kapsamında sistem dışından gelecek saldırıları izlemek ve engellemek.

- Kablosuz Algılayıcı Ağların (KAA) paket güvenliğini sağlamak ve dışarıdaki diğer ağlardan gelen isteklerde veriye doğrudan ulaşılmasını engellemek, bunu yaparken düşük maliyetli ve hızlı bir şekilde verilerin aktarılmasını sağlamak.
- Proje tüm internete bağlı tüm IoT cihazları için uygulanacağı için uygulama alanı geniştir. Ev, çevresel ortamlar, endüstri merkezler vb. Bu projede tüm IOT cihazlarından çıkan verinin şifrelenmesinin aynı olduğu kabul edilmiştir.

1.5. Projenin performans göstergeleri

Siber Güvenlik Sistemleri ile ilgili yapılacak projelerin performans göstergeleri aşağıdaki gibidir:

- Kullanılacak donanımların sayıları.
- IOT cihazlarının yönetilebilirliği.
- Merkezi sistem ile donanımlar arasında iletişim süresi.
- Alarm görüntüleme.
- Kontrolsüz geçiş alarm sayısı.
- İhbarların doğrulama süresinin azalması.
- Suç oranının düşmesi.
- Olası siber saldırılara karşı istikrarı koruması.

2. Proje Kapsamı ve Gerekçe

2.1. Proje Kapsamı

Boyd Cohen tarafından akıllı şehirlerin bileşenlerini konu alarak şematize edilmiş olan döngüden hareketle akıllı şehirleri meydana getiren bileşenler akıllı insan, akıllı çevre, akıllı yaşam, akıllı yönetişim, akıllı ekonomi ve akıllı ulaşım olarak belirlenmiştir. Bu bileşenler kendi içlerinde alt kırılımlara sahiptir ve akıllı şehrin meydana gelmesinde rol oynayarak birbirleriyle bütünleşmiş bir ekosistem oluştururlar [1]. Diğer çalışmalarda akıllı bir şehrin bileşenleri olarak güvenilir enerji ve su tedariki, şehir içi ve şehirler arası ulaşımın iyi olması, yönetimin etkin ve verimli olması, kamusal verilere 7/24 erişimin kolay olması, sosyal sermaye, yarışmacı ve rekabetçi bir üretim ve açık yerel ekonomi de belirtilmektedir. Bu nedenle akıllı şehir kavramı, ekonomi, ulaşım, çevre, insan, yaşam, yönetim ve denetimi içine alan kapsamlı bir yapıya sahiptir.

Akıllı Şehir Siber Güvenlik Sistemleri projesi ile akıllı şehir uygulamasında yer alacak tüm IoT cihazlarının verileri tek bir merkezde toplanarak takip edilecek, güncellenecek, yönetilecek ve güvenlikleri sağlanacaktır. Bu doğrultuda, Siber Operasyon Merkezi kurulacak ve IoT cihazlarından gelen verilerin güvenliği için IoT Güvenli Haberleşme modülleri kullanılacaktır.

Proje süresi, kurulum yapılacak alanın büyüklüğü ve kurulacak donanımların sayısına bağlı olarak belirlenir. Proje kapsamında 1000 hektarlık bir akıllı şehir proje uygulama alanı kurulacak ve bu alanda IoT cihazlarının kullanımı planlanmaktadır (Örneğin, akıllı aydınlatma, akıllı çöp toplama sistemi). Siber Operasyon Merkezi kurulduktan sonra güvenlik analizleri yapılacak, öncelik verilecek ihlaller ve riskler belirlenecek ve bu doğrultuda ne kadar bir yatırım yapılması gerektiği hesaplanacaktır. Maliyet kalemleri kullanılarak toplam bir bütçe belirlenecektir. Proje süresi ve maliyet, proje boyutuna ve kurulum detaylarına göre değişebilir.

2.2. Proje Gerekçesi

Akıllı şehirleşme sürecinde, nesnelerin interneti önemli bir konudur. Bu, birbirine bağlı fiziksel ve sanal nesneleri entegre eden, işbirliği yapabilen bilgi ve iletişim teknolojilerine dayanan bir altyapıdır. Kentlerdeki eksik hizmetlere çözüm getirmek amacıyla, cihazlar, sensörler, iletişim ağları, bulut sistemleri ve yazılımları içeren bir dizi teknoloji geliştirilmektedir.

Nesnelerin interneti, cihazların birbiriyle sürekli iletişimde olmaları nedeniyle potansiyel güvenlik riskleri barındırmaktadır. Bu cihazlar arasındaki kablosuz internet güvenliği, veri alışverişinin güvenliğinde kritik bir rol oynamaktadır. Bu proje, nesnelerin interneti sisteminin ve dolayısıyla akıllı şehrin güvenliğinin sağlanmasını amaçlamaktadır.

Aşağıda akıllı şehirlerde uygulanacak Siber Güvenlik Sistemleri projeleri için amaç ve hedefler sıralanmaktadır:

Amaçlar:

- Akıllı Şehir Siber Güvenlik Sistemleri ile siber saldırıları önlemeye çalışmak
- Olası siber saldırılarla ortaya çıkacak maddi hasarların önüne geçilmesi
- Güvenli veri alışverişinin sağlanması

Hedefler:

- Akıllı şehir kapsamında kullanılan IoT cihazlarının veri güvenliği sağlanmalıdır.
- Kablosuz Algılayıcı Ağların (KAA) paket güvenliği ve dış ağlardan gelen isteklere erişim engellenmelidir.
- Siber güvenlik saldırıları önlenmeli ve veri trafiğinin güvenliği sağlanmalıdır.
- IoT cihazlarından gelen şifreli verilerin güvenli bir şekilde takip ve izlenmesi gerekmektedir.
- Dış tehdit unsurlarından kaynaklanan IoT ve diğer cihazların veri güvenliği sağlanmalıdır.
- Siber Operasyon Merkezi ile oluşabilecek siber saldırılar izlenmeli ve önüne geçilmelidir.
- Sertifikasyon bilgisine sahip olmayan diğer ağlardaki istemcilerin algılayıcılara erişimi engellenmelidir.

- IoT cihazlarının merkezi sistem ile güvenli bağlantıları sağlanmalıdır.

2.3. Mevcut Durum

Proje konusu ile ilgili dünyada mevcut durumun tespiti

- Siber güvenlik uygulamalarına yönelik dünyadaki güncel eğilimler incelenir.
- Bu eğilimlere bağlı güncel teknoloji, yazılım, otomasyon, ekipman, yapı, ürün vs. incelenir.

Proje konusu ile ilgili Türkiye'de mevcut durumun tespiti

- Türkiye'deki mevcut siber güvenlik uygulamaları incelenir.
- Proje için gerek duyulan alanlarda hizmet alınabilecek firmalar belirlenir.

Daha önce yapılan çalışmaların başarı-başarısızlık durumlarının tespiti

- Bu uygulamaları gerçekleştiren kurum ve firmalarla bilgi, tecrübe, fikir alışverişi yapılır.
- Başarılı uygulamalar arasında kıyaslama yapılarak bölge için en uygun teknoloji, yapı, ekipman, otomasyon, yöntem ve ürün belirlenir.
- Süreç içerisinde karşılaşılan olumlu ve olumsuz durumlara dair bilgi notları hazırlanır ve bu notlarla bir bilgi havuzu oluşturulur.

Literatür Araştırması

Projeyi uygulamak isteyenler için hem dünyadan hem de Türkiye'den örneklere aşağıda yer verilmektedir:

Dünyada Siber Güvenlik Kavramı ve Uygulamaları

Akıllı şehir, şehirdeki farklı işlevleri birleştirerek yaşam kalitesini artırmayı hedefleyen bir yapıdır [2]. Yeni teknolojiler sayesinde şehir yaşamını kolaylaştırmak ve iyileştirmek mümkündür. Ayrıca teknoloji, kentsel hizmetlere operasyonel düzeyde katkı sağlamak ve faaliyet verilerini tutmak için kullanılmaktadır. Lim ve Malio çalışmalarında akıllı kentlerde ortaya çıkan işlevleri 5C (bağlantılılık/connection, biriktirme/collection, hesaplama/computation, iletişim/communications ve birlikte üretim/co-creation) ile formüle etmektedir [3]. Nesnelerin interneti uygulamaları sayesinde bağlantılılık sağlanırken, veriler toplanarak biriktirilir. Verilerin anlaşılır hale gelmesi için hesaplama ve özel algoritmalara ihtiyaç vardır. Akıllı şehirlerde sağlanan birlikte üretimle, hizmet sağlayıcılar ve tüketiciler bir araya gelerek değer yaratır. Bu gelişmeler, akıllı şehirlerin büyük veri potansiyeline vurgu yapmasına ve veri odaklı şehirleşme (data-driven urbanism) kavramının ortaya çıkmasına neden olur [4].

Akıllı şehirlerde büyük veri potansiyeli ve IoT cihazlarından gelen verilerin güvenliği önemli bir güvenlik ihtiyacı oluşturmaktadır. Bu ihtiyacı karşılamak için Siber Operasyon Merkezleri kurularak verilerin güvenli bir şekilde toplanması, analiz edilmesi ve raporlanması sağlanabilir. Bu merkezler sayesinde akıllı şehirlerdeki siber güvenlik önlemleri alınabilir.

Dubai Siber Güvenlik Merkezi, açık kaynak kodlu veri tabanlarının artan kullanıcıları ve olası güvenlik ihlalleri ile siber tehditlere karşı dijital güvenlik altyapısı sağlayarak kurumların ve kişilerin bilgilerini korumayı amaçlamaktadır. Birleşik Arap Emirlikleri'nde gerçekleşen siber güvenlik saldırılarının artması, Dubai E-Güvenlik Merkezi'nin 2014 yılında kurulmasına yol açmıştır. Bu merkez, iletişim ve bilgi sistemi ağlarının korunması ve koordinasyonunu sağlamaya odaklanmıştır. Dubai'nin akıllı şehir uygulamaları şehir güvenliği alanında birçok kazanım elde etmiş ve açık veri sisteminin yönetilebilirliğine katkı sağlamıştır. Bilgi güvenliği politikalarının belirlenmesinde de önemli bir rol oynamaktadır. Akıllı şehir uygulamalarının şehirsel güvenlik alanında katkı sağlaması nedeniyle bu tür uygulamaların yaygınlaşacağı söylenebilir [5].

Türkiye'deki Siber Güvenlik Uygulamaları

İstanbul Büyükşehir Belediyesi tarafından geliştirilen iTaksi Yönetim Sistemi, şehirde taksi kullanan vatandaşların seyahat deneyimini kolaylaştırmayı ve güvenli hale getirmeyi hedeflemektedir. Bu sistem, araç içi kameralar ve panik butonu gibi güvenlik önlemlerini içermektedir. Araçlarda bulunan kameralar sayesinde son bir haftaya ait görüntüler şifrelenerek saklanmakta ve vatandaşların kişisel verilerinin korunması sağlanmaktadır. Aynı zamanda, panik butonu sayesinde vatandaşlar güvenlik sorunları durumunda hızlı ve etkili bir şekilde müdahale alabilmektedir. iTaksi Yönetim Sistemi'nin İstanbul şehir güvenliği alanında sağladığı kazanımlar oldukça önemlidir. Özellikle güvenlik sorunlarında anlık ve doğrulanabilir verilerin emniyet birimleriyle paylaşılabilmesi, güvenliğin daha etkin bir şekilde sağlanmasına katkıda bulunmaktadır. Vatandaşların kişisel verilerinin korunması ve güvenlik sorunları durumunda anında müdahale alabilme imkânı sunan panik butonu, vatandaşlara güvenli bir seyahat deneyimi yaşatmaktadır [6].

Akıllı şehir uygulamaları henüz yeni ve gelişmekte olan bir alan olmasına rağmen, iTaksi gibi örneklerin artmasıyla birlikte toplum tarafından benimsenmesi ve yaygınlaşması beklenmektedir. Bu tür uygulamaların gelecekte daha da gelişeceği ve şehirlerin güvenliği, konforu ve yaşam kalitesinin artırılmasına katkı sağlayacağı öngörülmektedir.

Afyonkarahisar Afet Bilgi Sistemi, şehir güvenliğini artırmak için kullanılan bir akıllı şehir uygulamasıdır. Bu sistem, afet durumlarında etkin afet yönetimini sağlamak ve kriz durumlarında şehrin güvenliğini korumak amacıyla geliştirilmiştir. Uygulama, coğrafi bilgi sistemi (CBS) tabanlı olup deprem haritaları,

yangına hassas alanlar, heyelan ve sel bölgeleri, helikopter pistleri gibi önemli bilgilerin ilgili kamu yöneticilerine ulaştırılmasını ve kullanılabilir hale getirilmesini sağlamaktadır.

Afyonkarahisar Afet Bilgi Sistemi sayesinde afet yönetimi ve şehir güvenliği alanında önemli kazanımlar elde edilmiştir. Sistemin entegrasyonu ve şehir güvenliğine sağladığı katkılar, akıllı şehir uygulamalarının önemli bir rol oynadığını göstermektedir. Bu şekilde, şehir güvenliği ve afet yönetimi alanında akıllı şehir uygulamalarının etkili bir şekilde kullanılabileceği vurgulanmaktadır [6].

Siber operasyon merkezlerinin dünya genelinde siber saldırılara karşı mücadele birimleri olarak kurulduğu ve vatandaşlara doğru bilgi akışı sağladığı görülmektedir. Bu projede, uzman ekiplerle çalışılarak teknik donanım ve altyapının güçlendirilmesi hedeflenmektedir. Güvenlik yazılım ve donanımlarının yerli ve milli olması, ülke menfaati ve güvenliği açısından önem taşımaktadır. Aynı zamanda uzman ekiple çalışmanın siber güvenlik ihlallerinin önüne geçmede etkili olduğu görülmektedir. Başarılı projelerin temelinde, esnek mimari yapıya sahip altyapı seçimi ve hızlı karar mekanizmalarının yer alması önemlidir. Böylece güncel teknolojilerden faydalanarak başarılı ve yönetilebilir projelerin hayata geçirilmesi mümkün olacaktır.

Projenin bağlantılı olduğu başlıca alanlar şunlardır:

- Akıllı Şehircilik
- Siber Operasyon Merkezi
- IOT Haberleşme Modülleri
- Yazılım
- Donanım
- Otomasyon Sistemleri
- Siber Güvenlik ve İzleme Sistemleri

2.4. İhtiyaç Analizi

Projeye duyulan ihtiyacı ortaya koyan verilerin incelenmesi

Bilgi ve iletişim teknolojilerindeki gelişmeler, yeni ihtiyaçları doğurmuştur. Güvenlik, bu ihtiyaçların öne çıkanlarından biridir. Teknolojinin ilerlemesiyle güvenlik anlayışı değişmiş; bilgi toplumu, bilgi işleme ve yönetme yeteneğiyle birlikte afet durumları, para kullanımı, trafik güvenliği gibi birçok alanda güvenlik ihtiyacını artırmıştır. Bu ihtiyaçları karşılamak için akıllı şehir uygulamaları, yenilikçi ve sürdürülebilir çözümler sunmaktadır.

Güvenlik, özellikle su, ulaşım ve enerji yönetimi gibi kamusal alanlarda yerel yönetimlerin sorumluluğundadır. Bu bağlamda, teknolojik altyapıya sahip akıllı şehir uygulamalarına olan ihtiyaç önemli hale gelmiştir. Akıllı şehir uygulamaları, şehir yapısını göz önünde bulundurarak vatandaşların

ve yönetimlerin güvenlik ihtiyaçlarına yenilikçi çözümler sunmakta ve kamu hizmetlerinde yeni bir yaklaşım benimsemektedir. Günümüzdeki teknolojik imkanlar, bu alanda daha etkin yönetim tekniklerinin gelişmesine katkı sağlayabilir.

Proje ile ilgili beklentiler ve paydaşlara sağlanan faydalar ile çözüm getirilen problem ve sıkıntıların tespiti

Akıllı şehir uygulamalarının temel kaynağı veridir. Aynı zamanda, şehrin çeşitli noktalarındaki bilgileri birbirine ve veri depolama merkezleri arasında iletmektedir. Özellikle açık kaynak veya açık veri tabanlı sistemlerde üretilen bu veriler, kontrol ve yönetim konusunda potansiyel bir tehdit oluşturabilmektedir. Türkiye'de 2016 yılında yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu gibi hukuksal düzenlemelere rağmen, şehirsel güvenlik sorunlarına yönelik yeni düzenlemelere ihtiyaç vardır. İyi bir veri yönetimi, bireysel ve şehirsel güvenlik açısından kritik bir öneme sahiptir.

Dijitalleşme ile gelen yenilikler, güvenlik konusunda kolaylıklar sağlarken aynı zamanda güvenlik açıklarını da beraberinde getirmektedir. Kurumsal yapılar ve vatandaşlar, kullandıkları dijital platformlarda etkili güvenlik sistemleri oluşturmak zorundadırlar. Akıllı şehirler, sadece kurumsal verilerin değil, aynı zamanda kişisel verilerin korunması ve olası güvenlik ihlallerinin önlenmesi konusunda da sorumluluk taşımaktadır. Akıllı şehir uygulamaları, toplumsal yaşamda ve şehir yönetimlerinde etkinliği artırmanın yanı sıra, özellikle veri kullanımına bağlı olarak ortaya çıkabilecek güvenlik ihlalleriyle başa çıkabilmek için çözümler üretmelidir.

Şekil 1. Akıllı şehir örneği [6]

Projenin başarılı olmasını sağlayacak güçlü yönlerin ve başarısızlığa neden olabilecek zayıf yönlerin tespiti

- **Güçlü Yönler**
    - Akıllı şehirlerde farklı teknolojik bileşenleri entegre ederek şehir genelinde bütünlük sağlaması
    - Büyük veri setlerini hızlı bir şekilde analiz edebilmesi
    - Güvenlik tehditleri konusunda bilgi paylaşımını kolaylaştırması
    - Fiziksel güvenliği (güvenlik kameraları, bariyerler vb.) ile dijital güvenliği (ağ güvenliği, siber tehdit algılama, vb.) entegre ederek kapsamlı bir güvenlik yaklaşımı sunması
- **Zayıf Yönler**
    - Zayıf ağ güvenliği ya da güncellemeyen yazılımların potansiyel siber kayıplara ortam oluşturması
    - Güvenlik kameraları gibi fiziksel bileşenlerin yeterli güvenliğinin sağlanmadığı durumlarda hacklenme gibi zafiyetlere açık olması
    - Kurulacak sistemlerin finansal olarak kısıtlamalara sahip şehirler için yüksek maliyetli olması

2.5. Talep Analizi

Proje ile üretilecek ürünlere ve/veya sunulacak hizmetlere yönelik mevcut talebin tespiti

Proje kapsamında Siber Operasyon Merkezi (SOM) kurulması planlanmaktadır. SOM ekibi için uygun donanımsal ve yazılımsal altyapı gereklidir. Bazı SOM ekipleri olayları analiz etmek için gelişmiş adli analiz, kripto analiz, ters mühendislik ve zararlı yazılım analizi yeteneklerine sahiptir.

SOM'u kurmak isteyen herhangi bir kurum ya da kuruluşun öncelikle kurma stratejisini belirlemelidir. Bu strateji, işletmeye özgü hedefleri ve yöneticilerin desteğini içermelidir. Aynı zamanda, bu merkezlerine gereken altyapının sağlanması gerekmektedir. SOM altyapısı, güvenlik duvarları, IPS/IDS, DLP, Endpoint Security ve SIEM sistemini içermelidir. SOM personeli için veri akışları, network kayıtları, cihaz logları ve ihtiyaca göre gerekli kayıtlar toplanmalıdır. SOM işlemleri, SIEM ve SOAR sistemlerini kullanarak kurumun cihaz ve sistemlerinden gelen log kayıtlarının analiz edilmesine ve uygun sonuçlar ile tepkilerin üretilmesine dayanmaktadır.

SOM, kurumun bilgi güvenliği sistemlerini kontrol ve analiz ederek siber güvenlik tehditlerine karşı korur. SOM ekibi, yönetici, güvenlik analistleri, güvenlik mühendisleri ve diğer BT personeliyle koordineli olarak çalışır.

Şekil 2. SOM'un işlevleri [5]

SOM'un çalışma adımları aşağıdaki gibidir:

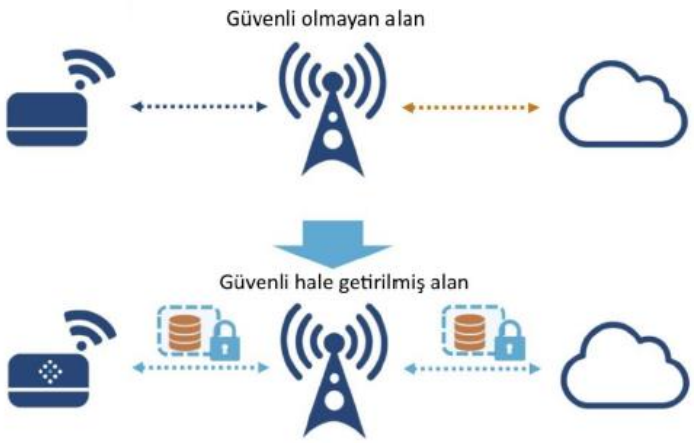
- Kurumun sahip olduğu sistemlerin, yazılımların ve donanımların tespiti.
- Tespit edilen envanterin zafiyet değerlendirmesinin yapılması.
- Sistemin sıradan ve sıradan dışı hareketlerinin belirlenmesi.
- IPS, IDS, DLP gibi teknolojiler kullanarak sızma ve sıradan olmayan hareketlerin tespit edilmesi.
- SIEM ve SOAR sistemlerinin kullanılması.
- Var olan saldırılara müdahale edilerek analiz yapılması ve sonuçların raporlanması.
- Raporlara göre güvenlik önlemlerinin alınarak sistemin daha güvenli hale getirilmesi.

Bu süreçte gerekli altyapıda aşağıdaki sistemlere ihtiyaç duyulmaktadır:

- IDS (Ağ trafiği içerisindeki zararlı hareketleri veya zararlı bağlantıların tespiti)
- IPS (Ağ trafiği içerisindeki zararlı hareketleri veya zararlı bağlantıların önlenmesi)
- DLP (Veri Kaybı/Sızıntısı Önleme Sistemi)
- Endpoint Security (Uç Nokta Güvenliği)
- SIEM (Güvenlik Olay Yönetimi ve Bilgi Toplama)
- SOAR (Güvenlik Düzenleme Otomasyon ve Yanıt)
- GRC Sistemleri (Risk Göstergeleri ve Erken Uyarı Sistemi)
- UTM (Yeni nesil Güvenlik Duvarı)

- NGFW (Üçüncü nesil Güvenlik Duvarı)

Ayrıca, IoT cihazlarından gelen verilerin şifrelenmesi için IoT cihazlarına entegre edilen Güvenli Haberleşme Modülü kullanılabilir. Bu modül, verileri AES 256-bit şifreleme algoritması kullanarak uçtan uca şifreler. Bu sayede veri güvenliği sağlanmış olur.



Şekil 3. Şifreleme sistemi olan ve olmayan güvenli-güvensiz alanların karşılaştırılması [5]

Talebin gelecekteki gelişim potansiyeli ve talep için gelecek öngörülerin tespiti

- Geleceğe yönelik nüfus, ekonomi ve teknoloji öngörüleri dikkate alınarak hesaplamalar yapılır.

3. Teknik Analiz ve Alternatif Teknolojilerin Değerlendirilmesi

Fiziki/Mekânsal Büyüklük

- Kurulması planlanan SOM'un büyüklüğü, kullanılacak IoT cihazlarının sayısı ile doğru orantılıdır. Bu nedenle kaç adet IoT cihazı olduğu ve kurulması planlanan SOM'un gereksinimleri projenin başında yapılacak kapsamlı ve detaylı bir analiz ile belirlenir.
- IoT cihazlarının sayısı ve SOM'un gereksinimleri doğrultusunda merkezin büyüklüğüne karar verilir.

Kapasitenin Belirlenmesi

- IoT cihazlarının sayısı ve SOM'un gereksinimleri doğrultusunda işlenmesi ve güvenliğinin sağlanması gereken verinin boyutu analiz edilir.
- Akıllı şehir uygulamaları verisinin gelecekte ulaşacağı boyut tahmin edilir.
- Analiz ve tahminler doğrultusunda SOM'un işlem kapasitesi ihtiyacı belirlenir.
- Belirlenen işlem kapsitesi için ihtiyaç duyulacak yazılım ve donanımlara karar verilir.

Yapısal Proje Gereksinimleri

- SOM’un projelendirilmesi
- SOM kapsamında ihtiyaç duyulacak donanımlar için gerekli olan yapının projelendirilmesi

Yazılım ve Donanım Gereksinimleri

Siber Güvenlik Sistemleri projesi için yazılım ve donanım gereksinimleri şunlardır:

- IDS (Saldırı Tespit Sistemi)
- IPS (Saldırı Engelleme Sistemi)
- DLP (Veri Kaybı/Sızıntısı Önleme) Sistemi
- Endpoint Securtiy (Uç Nokta Güvenliği)
- SIEM (Güvenlik Bilgileri ve Olay Yönetimi)
- SOAR (Güvenlik Düzenleme, Otomasyon ve Yanıt)
- GRC (Yönetişim, Risk ve Uygunluk) Sistemleri
- UTM (Birleşik Tehdit Yönetimi)
- NGFW (Yeni Nesil Güvenlik Duvarı)

Alternatif teknolojiler nelerdir? Karşılaştırma yapınız.

Siber güvenlik alanında evrensel bir yaklaşım ile SOM kurularak bu merkez aracılığıyla güvenlik sağlanır. Bu noktada iki adımlı bir yaklaşım bulunmaktadır. İlk aşamada gereksinimler analiz edilerek SOM tamamlanır. Devamında SOM’un gereksinimler doğrultusunda yazılım ve donanım ihtiyaçları karşılanır. Bu sayede SOM’un; ağlardaki, sunuculardaki, bitiş noktalarındaki, veri tabanlarındaki, uygulamalardaki, web sitelerindeki ve diğer sistemlerdeki etkinlikleri izlemesi ve analiz etmesi, bir güvenlik olayı veya tavizinin göstergesi olabilecek anormal etkinlikleri taraması, olası güvenlik sorunlarının doğru bir şekilde tanımlanması, analiz edilmesi, araştırılması ve rapor edilmesi sağlanır.

3.1. Siber Operasyon Merkezi (SOM)

Siber güvenlik operasyon merkezleri, ağlar, sunucular, bitiş noktaları, veritabanları, uygulamalar, web siteleri ve diğer sistemlerdeki etkinlikleri izleyen ve analiz eden birimlerdir. Anormal etkinlikleri tespit ederek güvenlik olayları veya tehditlerin belirtilerini tararlar. Bu merkezler, olası güvenlik sorunlarını doğru bir şekilde tanımlar, analiz eder, araştırır ve rapor eder. Böylece güvenliğin sağlanması ve olası tehditlere karşı önlem alınması sağlanır.

Bir Siber Operasyon Merkezi'nin etkin çalışması için; önemli bilişim sistemlerine ait logların sorunsuz bir şekilde analiz araçlarına iletilmesini sağlayacak güvenlik izleme cihazları ve altyapının düzenlenerek iyi bir şekilde yapılandırılması ve öğrenilmesi gerekmektedir. SOM kuralları düzenlenmeli ve zararlı aktiviteleri tespit etmek için alarmlar ve bildirimler araştırılarak önem derecesine göre sıralanmalıdır. Olay adımları önceden planlanmalı ve gerektiğinde bu plana uygun hareket edilmelidir. Gerçekleşen

saldırılarla ilgili inceleme ve kurtarma çalışmaları yapılmalı, adli analiz süreçleri gerçekleştirilmeli ve dersler çıkararak güvenlik önlemleri güncellenmelidir. İzleme ve tespit sistemlerinden elde edilen sonuçlara göre gerekli önlemler alınmalı ve politikalar güncellenmelidir.

Siber güvenlik operasyon merkezi ekiplerinde, tüm üyelerin misyon ve strateji konusunda farkındalığı sağlamak için etkili bir liderlik büyük önem taşır. Siber güvenlik operasyon merkezi yöneticisi, ekibi kurma ve motive etme konusunda yetkin olmalıdır. 7/24 çalışma gerekliliği stresli bir ortam yaratabilir ve bu da olası bir risk faktörüdür.

Siber Operasyon Merkezi (SOM) altyapısında kullanılan ürünler, güvenlik duvarları, IPS/IDS, DLP, Endpoint Security, SIEM Sistemi ve benzeri olarak sıralanabilmektedir. Bu ürünler, hizmet verilen kurum veya kuruluşa ait logların analiz edilmesini, iç ve dış siber olayların anlık olarak veya tehdide dönüşmeden önce engellenmesini sağlayan fiziksel ve yazılımsal bileşenler bütünüdür.

Siber Operasyon Merkezi (SOM) personelinin veri etkinliklerini ilişkilendirebilmesi ve analiz edebilmesi için veri akışları, network kayıtları, cihaz logları ve ihtiyaç duyulan diğer kayıtların toplanması gereklidir. SOM işlemleri, kurumun cihaz ve sistemlerinden gelen log kayıtlarını kullanarak dijital hareket verilerini analiz eden ve uygun sonuçlar ile tepkiler üreten SIEM ve SOAR sistemlerine dayanmaktadır.

Siber Operasyon Merkezi (SOM), kurumun bilgi güvenliği sistemlerini kontrol eden ve siber güvenlik tehditlerini analiz ederek koruyan bir ekipten oluşmaktadır. SOM ekibi, yönetici, güvenlik analistleri, güvenlik mühendisleri ve diğer BT personeliyle koordineli bir şekilde çalışır.

Siber Operasyon Merkezi (SOM) çalışma adımları şu sıra ile gerçekleşmektedir: İlk olarak, bölgedeki sistemlerin, yazılımların ve donanımların tespiti yapılır. Ardından, envanterin zafiyet değerlendirmesi gerçekleştirilir. Sistemin sıradan ve sıra dışı hareketleri belirlenir. IPS, IDS, DLS gibi teknolojiler kullanılarak sızma ve sıra dışı hareketler tespit edilir. SIEM ve SOAR sistemleri kullanılarak veriler analiz edilir. Eğer saldırı tespit edilirse müdahale edilir ve analiz sonuçları raporlanır. Raporlara göre güvenlik önlemleri alınarak sistem güvenilirliği artırılır.

3.2. IOT Güvenli Haberleşme Modülü

Siber Operasyon Merkezi (SOM), marka bağımsız IoT cihazlarının güvensiz haberleşme protokollerini güvenli hale getirmeyi ve verilerin manipülasyonunu önlemeyi amaçlar. Veriler, özel şifreleme algoritmaları kullanılarak anlaşılamaz hale getirilir ve sadece alıcı tarafından deşifre edilebilir. SOM, toplanan verileri işler ve şifrelenmiş verileri uç birimlere aktarır. Ayrıca dış tehditlere karşı ağ trafiğini denetleyerek uç nokta modülünü koruyacak senaryolar oluşturur.

IoT ağındaki tüm uç noktaların tam envanterini tutan ağ izleme yazılımı kullanılarak, IoT cihazlarına ait bilgilerin izlenmesi mümkündür. Aynı zamanda, bu cihazların yazılım güncellemeleri uzaktan ve merkezi bir şekilde takibi sağlanabilmektedir.

Bu rehberlik kılavuzu ile önerilen proje tasarısına göre siber güvenlik sistemleri için yapılacaklar, bir siber operasyon merkezinin kurulmasını ve IoT cihazlarının güvenli bir şekilde veri aktarabileceği haberleşme modüllerinin kullanılmasını kapsamaktadır.

3.3. Proje için Önerilen Çözüm Mimarisi

Bu projede, donanımları destekleyen entegre bir merkezi yönetim platformunun kullanımıyla, güvenlik ihlallerinin tespit edilerek fiziksel güvenliğin korunması hedeflenmektedir. Platform, uygulama alanında öncelikle kontrol edilmesi istenilen IoT cihazlarını kapsayan Siber Güvenlik Sistemlerini daha verimli hale getirmek ve düşük maliyetli bakım/destek çalışmaları yapmak için kullanılacak donanımlarla iletişim kurarak, donanımların açılıp-kapanması ve çalışma durumları hakkında bilgi sağlamayı amaçlamaktadır. Bu sayede Siber Güvenlik Sistemleri daha akıllı ve yönetilebilir hale gelmektedir.

Projenin uygulanacağı alan belirlendikten sonra donanımların konumları plana göre fiziksel ve enerji altyapılarına dayalı olarak belirlenmelidir. Siber Operasyon Merkezi Platformu ise uygulamayı gerçekleştirecek belediyelerin bilgi sistemleri altyapısının bulunduğu merkezi bir yerde kurulmalı ve Bilgi İşlem Dairesi tarafından yönetilmelidir.

Siber Operasyon Merkezi (SOM) Ana Özellikleri

Siber Güvenlik Operasyonları Merkezi (Security Operations Center), bir organizasyonun güvenliğini sürekli olarak izleyen ve güvenlik olaylarının analizinden sorumlu olan bir bilgi güvenliği ekibinin bulunduğu merkezi bir yer veya tesis olarak tanımlanabilir. Bu ekip, teknolojik çözümleri kullanarak etkili süreç yönetimi yapar ve siber güvenlik olaylarını tespit ederek analizini sunar. Aynı zamanda siber saldırılara karşı tedbirler alır ve müdahale eder.

Siber Operasyon Merkezi (SOM), iyi tanımlanmış süreçlerle siber güvenlik olaylarını önlemeyi amaçlayan bir sistemdir. Profesyonel bir ekip tarafından yönetilen SOM, siber güvenlik olaylarını tespit, analiz ve yanıtlama aşamalarında çalışır. Sürekli olarak kurumun güvenlik durumunu izleyen ve iyileştirmek için organize olan SOM, ayrıntılı iş süreçleri ve prosedürlere sahiptir.

Siber Operasyon Merkezi (SOM) şirketi siber güvenlik tehditlerinden korumak için tehditleri belirleyerek, analiz ederek ve tepki vererek çalışır. SOM, bir kuruluşun BT altyapısını izler ve merkezi bir komuta merkezi gibi davranır. Her olay için SOM, nasıl yönetileceği ve nasıl tepki verileceği konusunda kararlar alır ve saldırıları önceden tespit etmeye yardımcı olur.

Güvenlik operasyonları merkezleri, güvenlik analistleri, güvenlik mühendisleri ve güvenlik yöneticilerinden oluşur ve güvenlik operasyonlarını denetleyen yöneticileriyle birlikte çalışır. Eskiden sadece büyük kuruluşlar için uygun görülen SOM sistemi, günümüzde daha küçük kuruluşlar tarafından da tercih edilmektedir. Hibrit bir yapıya sahip veya fiziksel bir tesis olmayan sanal bir ekip olarak da kurulabilen SOM'lar, yarı zamanlı kurum içi personel ve dış kaynak uzmanlarının bir kombinasyonunu kullanabilme olanağı sağlamaktadırlar.

Akıllı Şehirler Siber Güvenlik Sistemlerinde ihlallerle başa çıkmak için önerilen çözüm mimarisi, güvenli haberleşme modülleriyle donatılmış IoT cihazları aracılığıyla verilerin güvenli bir şekilde Siber Operasyon Merkezine iletilmesini içerir. Merkezdeki donanım ve yazılımlar siber güvenlik ihlallerini tespit eder ve alarm üretir, ardından güvenlik analiz mühendisleri tarafından incelenerek gerekli önlemler alınır. Ayrıca, IoT Analiz yazılımı arızalı cihazların tespiti ve güncellemelerin yapılmasına olanak tanır. Bu sayede Akıllı Şehirlerde siber güvenlikte daha etkili bir koruma sağlanır. Çözüm mimarisinin ana bileşenlerine *1.2. Proje Teknik Bileşenleri* başlığında yer verilmektedir.

Teknoloji seçiminin dayandığı kriterler nelerdir? Açıklayınız.

1) Teknoloji yeni mi?
2) Teknoloji yerli mi?
3) Teknoloji yerli değilse yerlileştirilebilir mi?
4) Akıllı şehir kapsamında belirlenen alanda kullanılan IoT Cihazlarının veri güvenliği nasıl sağlanır?
5) Kablosuz Algılayıcı Ağların (KAA) paket güvenliği nasıl sağlanır ve dışarıdaki diğer ağlardan gelen isteklerde veriye doğrudan ulaşılması nasıl engellenir?
6) Siber güvenlik saldırıları nasıl önlenir ve veri trafiğinin güvenliği nasıl sağlanır?
7) IoT cihazlarından gelen şifreli verilerin güvenli bir şekilde takip ve izlenmesi mümkün müdür?
8) Kablosuz Algılayıcı Ağların (KAA) paket güvenliğinin sağlaması ve dışarıdaki diğer ağlardan gelen isteklerde veriye doğrudan ulaşılması engellenebilir mi?
9) Dış tehdit unsurlarının IoT ve diğer cihazların veri güvenlikleri sağlanabilir mi?
10) Siber Operasyon Merkezi ile oluşabilecek siber saldırıların izlenmesi ve önüne geçilmesi mümkün müdür?
11) Sertifikasyon bilgisine sahip olmayan diğer ağlardaki istemcilerin algılayıcılara erişimi engellenebilir mi?
12) IoT cihazlarının merkezi sistem ile bağlantılarını güvenli bir şekilde yapması sağlanabilir mi?

Teknik tasarım süreçlerini (süreç tasarımı, makine-donanım, inşaat işleri, arazi düzenleme, yerleşim düzeni vb.) açıklayınız.

SOM'un fiziki büyüklüğü ve kullanılacak olan IoT cihaz adedi ile doğru orantılıdır. Akıllı şehirde yaklaşık olarak ne kadar adet IoT cihazı olduğu ve kurulması gereken Siber Operasyon Merkezi (SOC) gereksinimleri projenin başında yapılacak kapsamlı ve detaylı bir analiz ile belirlenmelidir. Bu çalışmanın da özellikle projenin tüm paydaşları ile birlikte yapılması gerekmektedir. Proje başında yapılacak detaylı bir finansal analizle öncelikler belirlenmeli ve önerilen merkezi sistemler içinden Finansal Analiz bölümünde verilen maliyet kalemleri çıkarılmalıdır. Gerçek proje bütçesi çıkarılırken önceliklere göre fazlar belirlenerek yatırımın aşamalı bir şekilde yapılması önerilir. Bu kapsamda öncelikle Siber Operasyon Merkezinin kurulması önerilmektedir. Bu kapsamda teknik tasarım süreçlerini Siber Operasyon Merkezinin fonksiyonları oluşturmaktadır:

- Kurumun sahip olduğu sistemlerin, yazılımların ve donanımların tespit edilmesi.
- Tespit edilen envanterin zafiyet değerlendirmesini yapılması.
- Sistemin sıradan hareketlerini ve sıradan dışı hareketlerini belirlenmesi.
- IPS, IDS, DLS gibi teknolojileri kullanarak sızma ve sıradan dışı hareketlerin tespitinin yapılması.
- SIEM ve SOAR sistemleri kullanılması.
- Saldırı varsa müdahale etmek ve analiz yapmak. Analiz sonuçlarını raporlanması.
- Raporlara göre güvenlik önlemi almak ve sistemi eskisinden daha güvenilir hale getirilmesi.

Bu fonksiyonların sağlanması amacı ile de IoT Güvenli Haberleşme Modülünün kurulması önerilmektedir. IoT Güvenli Haberleşme Modülünün bileşenleri teknik tasarım süreçlerine girdi oluşturmaktadır:

- IDS (Ağ trafiği içerisindeki zararlı hareketleri veya zararlı bağlantıların tespiti)
- IPS (Ağ trafiği içerisindeki zararlı hareketleri veya zararlı bağlantıların önlenmesi)
- DLP (Veri Kaybı/Sızıntısı Önleme Sistemi)
- ENDPOINT Securtiy (Uç Nokta Güvenliği)
- SIEM
- SOAR (Güvenlik Düzenleme Otomasyon ve Yanıt)
- GRC Sistemleri (Risk Göstergeleri ve erken uyarı sistemi)
- UTM (Yeni nesil Güvenlik Duvarı)
- NGFW (Üçüncü nesil güvenlik Duvarı)

4. Finansal Analiz

Şehirlerdeki güvenlik ihlalleri, farklı türlerde olabilmektedir ve bu ihlallerin etkileri çeşitlilik göstermektedir. İhlalleri tespit eden ve önleyen çeşitli sistemler ve teknolojiler mevcuttur, ancak her bir ihlalin potansiyel maliyeti ve etkisi farklıdır. Bu nedenle, güvenlik çözümlerinin mali faydalarını hesaplamak için, olumsuz etkilerin olası maddi zararlarını önceden tahmin etmek ve bunları hesaba katmak önemlidir.

Güvenlik ihlalleri, sadece maddi hasarla sınırlı kalmayabilir, aynı zamanda sosyal ve ekonomik sonuçlar doğurabilir. Şehir sakinlerinin güvenliği ve refahı ihlallerin önlenmesi açısından önemli bir faktördür. Özellikle can kaybına yol açabilen ihlaller, maddi hesaplamalarla ölçülemeyecek büyük zararlara neden olabilir ve bu da şehir yönetimlerini bu tür olayları engellemek için önlem almaya zorlar.

Ancak, şehir yönetimleri sınırsız kaynaklara sahip değillerdir ve bütçeleri sınırlıdır. Bu nedenle, tüm güvenlik risklerinin tamamen ortadan kaldırılması pratik olarak mümkün olmayabilir. Bu durumda, şehir yönetimleri risklerin önem düzeylerini iyi değerlendirmeli ve bir risk / fayda analizi yaparak hangi ihlallere karşı öncelikli olarak önlem alacaklarını belirlemelidirler. Böylece mevcut kaynakları en etkin şekilde kullanarak şehir güvenliğini en iyi şekilde sağlayabilirler.

Örnek Vaka:

Finansal analiz kapsamında yatırım bütçesi, işletim maliyetleri ve gelirler belirlenerek yatırımın geri dönüş süresi tespit edilmelidir. **200.000 kişi**nin yaşadığı, **65.000 daire** bulunduran, **1000 hektar**lık alanı kapsayan bu projede, IoT (Nesnelerin İnterneti) uç noktalarının sayısı belirli olmamakla birlikte, her bir IoT uç noktası için Güvenli Haberleşme Modülü kullanılması planlanmaktadır. Proje alanının analiz edilmesi ve ihtiyaçlara göre IoT uç nokta sayısı yeniden belirlenebilir. Şu an için maliyet hesaplaması, 1000 adet IoT uç noktası üzerinden yapılmıştır. Ancak, IoT uç noktalarının tam sayısı kesinleştiğinde, Siber Operasyon Merkezinde kullanılacak yazılım ve donanımların hesaplaması yapılacaktır. Bu şekilde projenin uygulanması için gerekli kaynaklar ve maliyetler daha kesin bir şekilde belirlenecektir.

Akıllı şehirlerde siber güvenlik çözümlerinin temel maliyet kalemleri aşağıdaki gibidir:

Tablo 1. Siber güvenlik çözümlerinde temel maliyet kalemleri

Ürün	Açıklama	Fiyat Aralığı (USD)
Plan harita altyapısı	Diğer projelerle değerlendirilecektir.	
Siber Operasyon Merkezi (SOM) Kurulumu	SOM Merkezi (Donanım + Yazılım)	5.000.000 - 8.000.000
IDS (Ağ trafiği içerisindeki zararlı hareketlerin veya zararlı bağlantıların tespiti)*	SOM Yazılımı	*
IPS (Ağ trafiği içerisindeki zararlı hareketlerin veya zararlı bağlantıların önlenmesi)*	SOM Yazılımı	*
DLP (Veri kaybı/ sızıntısı önleme sistemi)*	SOM Yazılımı	*
ENDPOINT Security (Uç nokta güvenliği)*	SOM Yazılımı	*
SIEM*	SOM Yazılımı	*
SOAR (Güvenlik düzenleme otomasyon ve yanıt)*	SOM Yazılımı	*
GRC Sistemleri (Risk göstergeleri ve erken uyarı sistemi)*	SOM Yazılımı	*
UTM (Yeni nesil güvenlik duvarı)*	SOM Donanım + Yazılım	*
NGFW (Üçüncü nesil güvenlik duvarı)*	SOM Donanım + Yazılım	*
IoT Güvenlik haberleşme modülü	IoT Donanım + Yazılım	1.000.000 - 1.500.000
Siber Güvenlik Altyapısı*		*

ÖNEMLİ NOT: Proje uygulama alanında yapılar ve kullanılacak alanlar net olmadığı için, sayılar daha sonra netleşecektir. Dolayısıyla, 1000 hektar alanda **1250 adet IoT uç nokta** olacak şekilde birim fiyat verilmiştir.

Kurulum için gerekli kablolama, kurulum ekipmanları ve kurulum maliyetleri burada hesaplanmamıştır.

Bütçe: Bunların birçoğunun miktarının belirlenmesi için proje planının 1. maddesindeki veriler netleştiğinde toplam bütçe belirlenecektir.

*** İşaretli modüllerin detaylı bütçelemesi için projenin uygulanacağı alanın detaylı analizi gerekmektedir.**

Akıllı şehirlerde Siber Güvenlik Sistemlerinin ana bileşenleri aşağıda sıralanmaktadır:

- Plan harita altyapısı
- Siber Operasyon Merkezi (SOM) Kurulumu
- Kurulum maliyetleri
- IDS (Ağ trafiği içerisindeki zararlı hareketlerin veya zararlı bağlantıların tespiti)*
- IPS (Ağ trafiği içerisindeki zararlı hareketlerin veya zararlı bağlantıların önlenmesi)*
- DLP (Veri kaybı/ sızıntısı önleme sistemi)*
- ENDPOINT Security (Uç nokta güvenliği)*
- SIEM*
- SOAR (Güvenlik düzenleme otomasyon ve yanıt)*
- GRC Sistemleri (Risk göstergeleri ve erken uyarı sistemi)*
- UTM (Yeni nesil güvenlik duvarı)*
- NGFW (Üçüncü nesil güvenlik duvarı)*
- IoT Güvenlik haberleşme modülü
- Siber Güvenlik Altyapısı*

İşletim maliyetlerinin hesaplanmasında aşağıdaki temel parametreler göz önüne alınmalıdır.

- Yıllık Elektrik Tüketimi
- Yetkin Çalışan Maliyeti
- Donanım Bakım-Onarım Maliyetleri

Akıllı Şehir Siber Güvenlik Sistemlerinin geliştirilmesinde bazı Akıllı Şehir uygulamalarında da olduğu gibi maddi gelir sağlama motivasyonu bulunmamaktadır. Burada tüm Akıllı Şehir uygulamalarının güvenliğinin sağlanması temel motivasyon olup bu noktada kapsamlı bir ekonomik fayda yaratılmaktadır. Yaratılan ekonomik fayda, tehditlerin oluşturabileceği zararın önlenmesi ile elde edilen faydayı kapsamaktadır ve ekonomik fayda ilgili başlık altında detaylı bir şekilde açıklanmaktadır.

5. Ekonomik Analiz

Finansal faydanın yanında, Akıllı Şehir Siber Güvenlik Sistemleri projesi ile siber saldırıların önüne geçilmesi ve olası olumsuzlukların engellenmesi söz konusu olacaktır. Örneğin, aydınlatmada siber saldırı nedeniyle oluşabilecek olumsuzların önüne geçilmesi, vatandaşın huzur içinde yaşamasını da sağlamaktadır. Maddi hasarların ve kayıpların önüne geçilmesi için çözüm sunan proje ile başarılı ve huzurlu bir hayat yaşanması söz konusu olacaktır.

Oluşabilecek siber saldırılar sonucu meydana gelen doğrudan veya dolaylı finansal kayıpların (iş aksatma, finansal sektörlere yapılan saldırılar, bireysel bankacılık hedef alınarak yapılan saldırılar, şehir içi IoT cihazlara yapılan saldırılar vb.) önüne geçerek ekonomik anlamda fayda sağlayacaktır.

Siber saldırıların önüne geçilmesi, üretim ve finansal gibi siber saldırılardan en çok etkilenen sektörlerin olumsuz etkilenmesini de engeller. Böylece bu saldırıların, ülke içinde ve ülkeler arası finansal ve bilişim sektörünü olumsuz etkilemesi önlenirken, diğer yandan olası yatırımların gerçekleştirilmesinin önü açılır.

Siber saldırılara karşı koruyucu önlemlerin alınması, ülke/kurumların itibarlarının sürdürülmesini sağlar. Bu da ekonomik olarak itibarın uzun vadede ülkeye kazandıracağı maddi kazançlar olarak gözükebilir.

6. Sosyal Etkinin Analizi

IoT cihazlarına yapılabilecek siber saldırıların önüne geçilmesi, yaşam alanlarında vatandaşın güvende ve huzurla yaşamasını sağlar ve yaşayış şekillerini çeşitlendirir.

Proje şehri/bölgeyi istenilen yaşam halini getirecek ve yetkililerin istediği türden bir alan olması sağlayacaktır.

7. Çevresel Etkinin Analizi

Şehir içi güvenliğini sağlayan IoT cihazlarının stabil bir şekilde çalışması ve bu çalışmanın aksamaması çevresel güvenliğin sağlanmasına yardımcı olur.

8. Risk Analizi

Akıllı Şehir Siber Güvenlik Sistemlerinin geliştirilmesinin önünde risk teşkil eden konulara aşağıda örnekler verilmiştir. Bu örnekler kapsamında odaklanılan konulara yönelik ve bu örnekler haricinde siber güvenliğin sağlanmasına yönelik risk analizlerinin yapılması gerekmektedir.

- İlk yatırım maliyetinin caydırıcılığı ve uzun dönemdeki sağlanan faydanın belediyelerin anlık gereksinimleri karşısında ikinci plana itilmesi
- Projenin bir bütün olarak planlanmasına rağmen süreçte mali sıkışıklık durumunda kesintiye uğraması.
- Proje planına uyulmaması.
- Proje planını etkileyecek 3. Firmalar tarafından üstlenilmiş diğer alt yapı ve planlanan işlerin zamanında tamamlanmaması
- Mahalli İdarelerde Yönetim değişikliği ve buna bağlı projenin gecikmesi veya tam anlamı ile gerçekleşmemesi
- Ödemelere bağlı gecikmeler, ithal ürünlerin fiyatlarının artması
- Süreç içinde teknolojik ve ürün değişmelerine karşı uyumlu güncellemelerin yapılabilmesi
- Sistemin devreye girmesi ile bakım ve destek hizmetlerinin başlaması bu amaçla bir yapılanmanın mutlaka proje dahilinde düşünülmesi. İşletmeye alınacak yeni bölge ve ürünlerin de aynı yapılanma ile yürütülmesi
- İthalatta aksama ya da gecikme olması
- Ağ altyapısı ve IoT güvenlik modülleri kurulumlarında esnasında yanlış konumlandırma yapılarak, ilerleyen süreçte optimizasyon sürelerini uzatması
- Maliyet sebepli yeterli düzeyde olmayan veya mevcut donanım parkını karşılamaya uygun olmayan sunucu ve yazılım kurulumlarının yapılması

9. Genel Değerlendirme ve Sonuç

Son yıllarda güvenlik anlayışı, fiziki güvenlikten siber güvenliğe doğru evrim geçirmiştir. Bu değişimle birlikte teknolojinin hızlı gelişimi ve akıllı cihazların yaygınlaşmasıyla tehditlerin boyutu ve çeşitliliği artmıştır. Akıllı cihazların hayatımızın her alanında kullanılması, siber tehdit riskinin yaygınlaşmasına neden olmuştur ve bu tehditler, kişisel yaşam alanlarından üretim ve tüketim noktalarına kadar her alanda karşımıza çıkabilmektedir.

Projenin başlangıcında, tüm paydaşlarla kapsamlı bir ihtiyaç analizi çalışması yapmak kritik öneme sahiptir. Bu analizde eksik veya dahil edilmeyen paydaşlar, ileride ihlal tespitlerinde sorunlar yaşanmasına neden olabilir. İhtiyaç sahipleri ve teknoloji tedarikçileri arasında senaryolar ve kapasite konularına dikkat edilmeli ve kurulacak sistemlerin önemli ihlalleri tespit edebilecek düzeyde olması sağlanmalıdır. Optimum kapasite ve yatırımı planlamak için küçük alanlarda deneyim kazanarak kademeli bir yaklaşım benimsemek faydalı olabilir.

Teknoloji alanındaki gelişmeler sayesinde makine öğrenme ve yapay zekâ teknolojileri ile teknolojileri aldatmak daha zor hale gelmiştir. Ancak hiçbir teknoloji yüzde yüz performans gösteremez, bu nedenle benzer riskler hala varlığını korumaktadır.

Projeye özgü risklerin yanı sıra, genel proje risklerinin de ele alınması gerekmektedir. Akıllı Şehir Siber Güvenlik Sistemleri projesinde karşılaşılabilecek önemli risklerin belirlenmesi önemlidir ve bu risklerin yönetimi için uygun önlemler alınmalıdır.

Tablo 2: Proje riskleri ve dereceleri [5]

Risk Numarası	Risk	Olasılığı	Etkisi	Derecesi
1	İlk yatırım maliyetinin caydırıcılığı ve uzun dönemdeki sağlanan faydanın belediyelerin anlık gereksinimleri karşısında ikinci plana itilmesi	3	5	Yüksek (15)
2	Projenin bir bütün olarak planlanmasına rağmen süreçte mali sıkışıklık durumunda kesintiye uğraması.	2	4	Orta (8)
3	Proje planına uyulmaması.	4	4	Yüksek (16)
4	Proje planını etkileyecek 3. Firmalar tarafından üstlenilmiş diğer alt yapı ve planlanan işlerin zamanında tamamlanmaması	4	4	Yüksek (16)
5	Mahalli İdarelerde Yönetim değişikliği ve buna bağlı projenin gecikmesi veya tam anlamı ile gerçekleşmemesi	2	5	Orta (10)
6	Ödemelere bağlı gecikmeler, ithal ürünlerin fiyatlarının artması	3	4	Orta (12)
7	Süreç içinde teknolojik ve ürün değişmelerine karşı uyumlu güncellemelerin yapılabilmesi	3	3	Orta (9)
8	Sistemin devreye girmesi ile bakım ve destek hizmetlerinin başlaması bu amaçla bir yapılanmanın mutlaka proje dahilinde düşünülmesi. İşletmeye alınacak yeni bölge ve ürünlerin de aynı yapılanma ile yürütülmesi	2	4	Orta (8)
9	İthalatta aksama ya da gecikme olması	3	4	Orta (12)
10	Ağ altyapısı ve IoT güvenlik modülleri kurulumlarında esnasında yanlış konumlandırma yapılarak, ilerleyen süreçte optimizasyon sürelerini uzatması	3	4	Orta (12)
11	Maliyet sebepli yeterli düzeyde olmayan veya mevcut donanım parkını karşılamaya uygun olmayan sunucu ve yazılım kurulumlarının yapılması	4	4	Yüksek (16)

Risk analizinde gerçekleşme olasılıkları ve etkiler, 1 ila 5 arasında değerlendirilmiştir. Olasılıklar, çok düşük, düşük, orta, yüksek ve çok yüksek olarak kategorize edilmiştir. Etkiler ise çok az, az, orta, büyük

ve çok büyük olarak sıralanmıştır. Bu olasılık ve etkiler birlikte değerlendirilerek risklerin toplam derecesi belirlenmiştir. Dereceler, olasılık ve etkilerin çarpımı sonucu hesaplanmıştır ve aşağıdaki tabloda verilmiştir:

1. Çok düşük risk: Olasılık ve etki düşük (%0-20 arası)

2. Düşük risk: Olasılık düşük, etki orta (%20-40 arası)

3. Orta risk: Olasılık ve etki orta (%40-60 arası)

4. Yüksek risk: Olasılık yüksek, etki orta (%60-80 arası)

5. Çok yüksek risk: Olasılık ve etki yüksek veya çok yüksek (%80-100 arası)

Bu riskler ile yüzleşildiğinde aşağıdaki etkiler ile karşılaşılabilir:

1. Çok az etki: Gerçekleştiği takdirde fazla önemsenmeyecek veya çok az önemsenecek bir etki, örneğin projenin bitiş tarihini etkilemeyecek miktarda bazı aktivitelerin gecikmesi veya bütçeyi fazla etkilemeyecek şekilde maliyetlerde oynama.

2. Az etki: Gerçekleştiği takdirde hafif bir etki, örneğin projede az miktarda gecikmeler, maliyetlerde az artışlar.

3. Orta etki: Gerçekleştiği takdirde orta dereceli bir etki, örneğin projede orta miktarda gecikmeler, maliyetlerde küçük artışlar.

4. Büyük etki: Gerçekleştiği takdirde önemli derecede bir etki, örneğin projenin önemli derecede gecikmesi, maliyetlerde önemli artışlar.

5. Çok büyük etki: Gerçekleştiği takdirde ciddi derecede bir etki, örneğin projenin uzun bir süre durması ve iptal olması, maliyetlerde altından kalkılamayacak derecede artışlar.

Bu olasılıklar ve etkilere göre risk dereceleri numaraları birbiri ile çarparak belirlenir. Buna göre dereceler aşağıdaki tabloda verilmiştir.

Aşağıdaki tablo, proje yönetimi için risklerin öncelik sırasını belirlemek ve risk yönetim stratejilerini planlamak için kullanılabilir:

Tablo 3: Olasılık ve Etkisine Göre Risk Dereceleri [5]**Olasılık \ Etki**	**Çok az (1)**	**Az (2)**	**Orta (3)**	**Büyük (4)**	**Çok Büyük (5)**
Çok düşük (1)	Anlamsız 1	Düşük 2	Düşük 3	Düşük 4	Düşük 5
Düşük (2)	Düşük 2	Düşük 4	Düşük 6	Orta 8	Orta 10

Orta (3)	Düşük 3	Düşük 6	Orta 9	Orta 12	Yüksek 15
Yüksek (4)	Düşük 4	Orta 8	Orta 12	Yüksek 16	Yüksek 20
Çok yüksek (5)	Düşük 5	Orta 10	Yüksek 15	Yüksek 20	Kritik 25

Günümüz teknolojisi, hayatın birçok alanında önemli bir rol oynamaktadır ve beraberinde ciddi riskler getirmektedir. Bu risklerle başa çıkabilmek için teknolojinin korunması, izlenmesi ve denetiminin anlık olarak yapılması gerekmektedir. Bu projede amaç, hedeflenen lokasyonda siber güvenliğin en üst düzeye çıkarılmasını sağlamak ve faaliyetlerin kesintisiz devam etmesini temin etmektir.

10. Kaynakça

[1] Soe, R. (2017). FINEST twins: Platform for cross-border smart city solutions. *The 18th Annual International Conference*. https://doi.org/10.1145/3085228.3085287

[2] *About us- Dubai Electronic Security Center (DESC)*. (2020, October 12). DESC. https://www.desc.gov.ae/about-us/

[3] Nuaimi, E., Al-Neyadi, H. A., Mohamed, N. ve Al-Jaroodi, J. (2015). Applications of Big Data to Smart Cities. Journal of Internet Services and Applications, 6 (25), 1-15.

[4] Lim, C., Kim, K.-J. ve Maglio, P. P. (2018). Smart Cities with Big Data: Reference Models, Challenges and Considerations. Cities, 82, 86-99 / Data-Driven Understanding of Smart Service Systems Through Text Mining. Service Science, 10 (2), 154-180

[5] Kitchin, R. (2016). The ethics of smart cities and urban science. Phil.Trans.R. Soc., 1- 15, http://dx.doi.org/10.1098/rsta.2016.0115.

[6] TÜBİTAK- TÜSSİDE. (Nisan 2021). Esenler Belediyesi Akıllı Şehir Uygulamaları Fizibilite Projesi. Siber Güvenlik Sistemleri Ön Fizibilite Raporu.