İSTANBUL BİLGİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
BİLİŞİM VE TEKNOLOJİ HUKUKU YÜKSEK LİSANS PROGRAMI

AKILLI ŞEHİRLERDE SİBER GÜVENLİK

Özgür ALP
115691007

Prof. Dr. Ahmet DENKER

İSTANBUL
2018

AKILLI ŞEHİRLERDE SİBER GÜVENLİK

CYBER SECURITY IN SMART CITIES

Özgür ALP

115691007

Tez Danışmanı:	**Prof. Dr. Ahmet DENKER** İstanbul Bilgi Üniversitesi	(İmza) .....
Jüri Üyeleri:	**Doç. Dr. Üyesi Leyla KESER** İstanbul Bilgi Üniversitesi	(İmza) .....
	Dr. Öğr. Üyesi Mehmet Bedii Kaya Yıldırım Beyazıt Üniversitesi	(İmza) .....

Tezin Onaylandığı Tarih : 22.06.2018

Toplam Sayfa Sayısı : 91

Anahtar Kelimeler (Türkçe)	Anahtar Kelimeler (İngilizce)
1) Akıllı Şehir Teknolojileri	1) Smart City Technologies
2) Nesnelerin İnterneti	2) Internet of Things
3) Siber Güvenlik	3) Cyber Security
4) Siber Zayıflıklar	4) Cyber Weaknesses
5) Siber Saldırılar	5) Cyber Attacks

İÇİNDEKİLER

ŞEKİL LİSTESİ

TABLO LİSTESİ

ABSTRACT

As our world is getting digitalized, all the tools and devices we use in our daily lives are beginning to integrate with technology. As technological developments increase in individual and social level, systems and services that work together are emerged. The combination of these systems and services creates smart cities that have been integrated to make our daily life easier.

Smart city technologies are used to measure city-related risks and manage uncertainties. Many different smart city technologies, especially used in transportation, energy, environment, construction, infrastructure, public service, health and agriculture, increase productivity.

Systems and services are connected to each other and internet through a network in order to work integrated with each other. A system which is connected to any network, security risks are beginning to occur. As the digitalization increases in areas where smart city technologies are used, the cyber-attack surface in network, server and application layer levels expands and creates different security vulnerabilities that need to be managed and resolved. In order to manage and resolve these vulnerabilities, cyber vulnerabilities in smart city technologies should be explored.

In this research, cyber security vulnerabilities, which are likely to be found in smart city technologies, will be reviewed with various attack scenarios and a roadmap proposal will be presented to enable cyber security in smart city technologies.

In the first chapter, smart city concept will be mentioned in general, smart cities will be defined and their characteristics will be examined. In the second chapter, city of Copenhagen in Denmark will be examined as an example smart city. In the third chapter, technologies used in smart cities will be mentioned. In the fourth chapter, cyber world and cyber security will be introduced. In the fifth chapter issues need to be taken into consideration about cyber vulnerabilities will be

described. In the sixth chapter, the possible effects of the cyber-attacks will be seen through the attack scenarios that likely take place in the smart cities. In the seventh chapter, the security principles, traditional, legal and modern solutions to be followed in the way of being a secure and smart city will be suggested.
Keywords: Smart City Technologies, Internet of Things, Cyber Security, Cyber Weaknesses, Cyber Attacks

ÖZET

Dünyamız dijitalleştikçe, gündelik hayatımızda kullandığımız araçların hepsi teknoloji ile entegre olmaya başlamaktadır. Teknolojik gelişmeler bireysel ve toplumsal seviyede arttıkça, birbiri ile entegre çalışan sistemler ve servisler oluşmaktadır. Bu sistemlerin ve servislerin birleşimi ise, gündelik hayatımızı kolaylaştırmak için entegrasyonu sağlanmış akıllı şehirleri oluşturmaktadır.

Akıllı şehir teknolojileri, şehir ile ilgili riskleri ölçmek ve belirsizlikleri yönetmek için kullanılmaktadır. Özellikle ulaşım, enerji, çevre, inşaat, altyapı, kamu hizmeti, sağlık ve tarım alanlarında kullanılan birçok farklı akıllı şehir teknolojisi verimliliği arttırmaktadır.

Sistemler ve servisler, birbiri ile entegre çalışmak için bir ağ üzerinden birbirlerine ve internete bağlı hale gelmektedirler. Herhangi bir ağa bağlı olan bir sistemde, güvenlik riskleri oluşmaya başlamaktadır. Akıllı şehir teknolojilerinin kullanıldığı alanlarda dijitalleşme arttıkça; ağ, sunucu ve uygulama katmanı seviyelerinde siber saldırı yüzeyleri genişlemektedir ve yönetilmesi ve çözülmesi gereken farklı güvenlik açıklıkları oluşmaktadır. Bu güvenlik açıklıklarının yönetilmesi ve çözülebilmesi için, akıllı şehir teknolojilerinde bulunan siber zayıflıklar incelenmelidir.

Bu araştırmada, akıllı şehir teknolojilerinde bulunma ihtimali olan siber güvenlik açıklıkları, çeşitli saldırı senaryoları ile birlikte incelenecek, akıllı şehir teknolojilerinde siber güvenliğin sağlanabilmesi için bir yol haritası önerisi sunulacaktır. Birinci bölümde genel olarak akıllı şehir konseptinden bahsedilecek, akıllı şehirlere bir tanım yapılacak ve özellikleri incelenecektir. İkinci bölümde örnek bir akıllı şehir olan Danimarka'nın Kopenhag şehri incelenecektir. Üçüncü bölümde akıllı şehirlerde kullanılan teknolojilerden bahsedilecek, dördüncü bölümde ise siber dünya ve siber güvenlik konularına giriş yapılacaktır. Beşinci bölümde siber zayıflıklar konusunda dikkat edilecek konulara değinilecek, altıncı bölümde ise akıllı şehirlere gerçekleşecek saldırı senaryoları üzerinden, saldırıların

olası etkileri görülecektir. Yedinci bölümde güvenli akıllı şehir olma yolunda izlenmesi gereken güvenlik prensipleri, geleneksel, yasal ve modern çözüm önerilerinde bulunulacaktır.

Anahtar Kelimeler: Akıllı Şehir Teknolojileri, Nesnelerin İnterneti, Siber Güvenlik, Siber Zayıflıklar, Siber Saldırılar

BİRİNCİ BÖLÜM

AKILLI ŞEHİRLERE GİRİŞ

1.1. AKILLI ŞEHİR NEDİR?

Şehirler, dünya nüfusunun büyük çoğunluğunun yaşadığı, geçimini sağladığı ve hizmet aldığı yerleşim birimleridir. Dünya nüfusunun büyük bir çoğunluğu şehirlerde ikamet etmektedir. Birleşmiş milletlerin 2016 yılında yayınladığı rapora göre, dünya nüfusunun yaklaşık yüzde 54,5'lik bölümü şehirlerde yaşıyor. Aynı rapora göre 2030 yılı itibariyle bu sayı, dünya nüfusunun yüzde 60'lık bölümünü kapsayacak. (United Nations, 2016)

Nüfusun çoğunluğuna ev sahipliği yapmasının ve her geçen yıl çoğalan nüfuslarının katlanarak artmasının sonucu olarak şehirlerde, ulaşım, sağlık ve enerji gibi hizmetlerin aksamadan sağlanması büyük bir önem arz etmektedir.

Son yıllarda bilgi teknolojilerinde yaşanan çığır açıcı yeniliklerin sonucu olarak, hayatımızı kolaylaştıran ürünlerin "akıllanmaya" başladığı görülüyor. Özellikle nesnelerin interneti, bulut mobil bilişim konseptleri ile birlikte kullandığımız cihazların değişikliklere uyum sağlayabileceği, birbirleriyle haberleşebileceği ve çevrelerindeki değişiklikleri hissedebileceği bir şekilde evrimleştiğine tanık olmaktayız. Bu gelişmeler, hayatımızın her alanını etkilediği gibi, şüphesiz ki insanların yaşam alanlarını da etkileyecektir.

Geleneksel şehir altyapısının, artan şehir nüfusuyla birlikte yetersiz kalması ve her geçen gün azalan kaynakların verimli bir şekilde kullanılmasının elzem bir durum haline gelmesi ile birlikte teknolojinin, yaşadığımız şehirlere yeni bir tanım getirmesi kaçınılmaz bir durum olmuştur. Teknolojinin, geleneksel şehir altyapısıyla entegre olması ve nesnelerin birbirleriyle bağlantılı bir ağ olarak çalışması sonucunda akıllı şehirler ortaya çıkmaya başlamıştır.

Literatürde net bir tanımı olmayan akıllı şehir kavramı, azalan kayakların daha verimli ve sürdürülebilir kullanılabilmesi, sağlık, ulaşım, güvenlik, eğitim gibi hizmetlerin daha etkili bir şekilde insanlara ulaştırılarak, şehirlerin daha yaşanabilir alanlar haline getirilme ihtiyacı ile birlikte doğmuştur. Bu ihtiyaçları karşılayabilen ve çağın getirdiği değişime ayak uyduran şehirler, birbirleriyle iletişim halinde çalışan sensörler, izleme ve ölçüm cihazları gibi elektronik cihazlarla donatılmaktadır.

Birçok bilimsel makalede farklı alternatif tanımlar halinde sunulan akıllı şehir tanımlardan bir tanesi akıllı şehirleri "Kritik altyapı bileşenlerinin ve kentsel yönetim, eğitim, sağlık, kamu güvenliği, gayrimenkul, ulaşım gibi kamu hizmetlerinin akıllı bilgi işlem teknolojileri kullanılarak, birbirine bağlı olarak daha akıllı ve daha verimli hale getirildiği şehirlerdir." (Washburn, et al., 2010) şeklinde tanımlamıştır.

Şekil 1 Akıllı Şehir Konsept Haritası

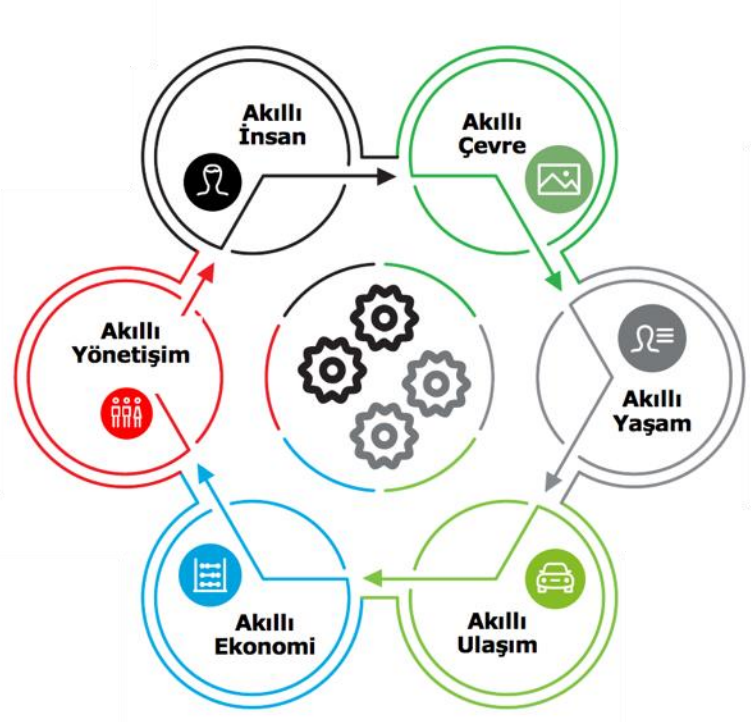
Şehirde verilecek olan hizmetlerin, şehir içerisinde birbirine bağlı çalışan, eş zamanlı izleme yapan, bilgi toplayan ve akıllı servisler sunan elektronik cihazlarla birlikte gerçekleştirilmesi ile, güvenlik ve mahremiyet kaygılarının oluşması kaçınılmaz bir sonuç olarak ortaya çıkmıştır.

Güvenlik ve mahremiyet ihtiyacının karşılanmasının kaçınılmaz olduğu da göz önüne alınarak, söz konusu şehirlerin "güvenli akıllı şehir" olarak tanımlanması ve akıllı şehirlerin bu çerçevede planlanması önem arz etmektedir.

1.1.1. Akıllı Şehirlerin Boyutlandırılması

Bir şehrin, akıllı şehir olarak tanımlanabilmesi için, sadece akıllı elektronik cihazlar ve yazılımlar olarak değil, etkilenen şehri her bileşeniyle değerlendirmek gerekmektedir. Akıllı şehirlerin beş temel bileşeni bulunmaktadır: Modern bilgi ve işlem teknolojileri, binalar, kamu hizmetleri ve altyapılar, ulaşım ve trafik kontrolü ve şehrin kendisidir. Ancak, sadece bu bileşenlere sahip olan şehirleri akıllı olarak tanımlamak mümkün değildir.

Akıllı şehirler 6 temel boyutta incelenebilir. Bunlar akıllı yönetişim, akıllı ekonomi, akıllı insanlar, akıllı ulaşım, akıllı yaşam ve akıllı çevredir (Aldairi & Tawalbeh, 2017)



Şekil 2 Akıllı Şehrin Boyutları

(Deloitte & Vodafone, 2016)

1.1.1.1. Akıllı Yönetişim

Şehrin tüm bileşenlerinin akıllı bir şekilde yönetilmesi, şeffaflığın ve mahremiyetin sağlanması bunların yanında teknolojinin toplumun yararına ve kaynakların akıllı bir şekilde kullanılması, güvenli akıllılaşma sürecinde kritik önem taşımaktadır. Bu boyutun bileşenleri özel, kamusal ve sivil örgütler, altyapı, hükümet ve kuruluşlardır.

1.1.1.2. Akıllı Ekonomi

Akıllı ekonomiler, bilgiye, teknolojiye, yenilikçi girişimlere dayanan; esnek ve global manada rekabetçi, katma değer üreten ve bunların yanında enerjiyi verimli kullanan ve yenilenebilir enerjiyi destekleyen paydaşlar üretebilen ekonomilerdir. (Kumar & Dahiya, 2017) Eldeki sermayenin verimli bir şekilde kullanıldığından emin olunması, yozlaşmışlık ve sahtekarlığın önüne geçilebilmesi için kullanılan sistemlerin güvenliğini sağlamak kaçınılmaz bir ihtiyaçtır. Bu boyutun bileşenleri e-ticaret, e-iş, üretim sektörü başta olmak üzere esasında ekonomiye doğrudan ve dolaylı olarak etki eden tüm sektör ve bileşenlerdir.

1.1.1.3. Akıllı Ulaşım

Günümüzdeki geleneksel ulaşım imkanları lojistik anlamda birçok soruna çözüm olsa bile, akıllı şehirlerle birlikte şehirlerdeki trafik yoğunluğu, trafik kazaları, gaz salınımı gibi birçok çözülmemiş soruna çözüm getirirken aynı zamanda mevcut ulaşımın hızlandırılması ve daha verimli hale getirilmesini amaçlar. Sadece fiziksel ürünlerin güvenle taşınması değil aynı zamanda dijital verilerin de güvenli bir şekilde taşınması hususunun da ele alınması gerekmektedir. Bu boyutun bileşenleri olarak şehir trafiği ve trafikteki bütün araçlar, trafiği düzenlemeye yardımcı olacak sensörler, lojistik sistemler, kablolu ve kablosuz ağlar gösterilebilir.

1.1.1.4. Akıllı Yaşam

İnsan odaklı bir kavram olan akıllı şehirlerin bir diğer amacı da yaşayan insanların refah seviyelerinin yükseltilmesidir. Akıllı şehirlerde yaşayan insanların hayatlarının daha verimli, güvenli, kontrol edilebilir, üretken, entegre ve sürdürülebilir olması beklenir. Güvenli akıllı şehir kavramıyla bu gelişme ve iyileşmeleri sağlayacak servislerin her gün ve her saat kesintisiz olarak verilmesini ve aynı zamanda bu servisleri sağlarken üretilen verilerin gizliliğinin korunduğundan emin olunur.

1.1.1.5. Akıllı İnsan

Teknolojik gelişmeler ve yenilenen ve geliştirilen sistemleriyle akıllı şehir insanlarının da özellikle teknolojiyi kullanabilecek, takip edebilecek ve değişime çabuk adapte olabilecek seviyede olması gerekmektedir. Şehir içerisindeki bütün insanlar ve eğitim kurumları bu boyutu oluşturan bileşenlere dahildir.

1.1.1.6. Akıllı Çevre

Doğaya karşı şehirleşme ile birlikte doğaya verilen zararı azaltmak ve yok etmek de akıllı şehirlerin hedefleri içerisindedir. Kaynakların kontrol altında tutulması ve verimli kullanılması, atıkların kontrol edilmesi ve geri dönüştürülmesi, doğaya duyarlı teknolojilerin kullanılması, enerji kaynağı olarak ağırlıkla yenilenebilir enerjilerin kullanılması amaçlanmaktadır. Bu boyutun bileşenleri olarak her türlü doğal kaynaklar, enerji, atık kontrol merkezleri gibi bileşenler sıralanabilir. Kaynaklar doğru ve verimli bir şekilde kullanılırken, faydalanılan sistemlerin güvenli bir hale getirilmesi kaynakların verimsiz ve boşa harcanmasını engellemek için hayati önem taşımaktadır.

Akıllı güvenli şehir konseptinde her bir boyut, sistemin değişmez parçası olarak görülmeli ve her bir boyutun güvenliği ayrı ayrı sağlanarak bir bütün halinde işleyebilir duruma getirilmelidir.

1.1.2. Akıllı Şehirlerin 3 Temel Aktörü

Nam ve Pardo akıllı şehir modellemesine göre (Nam & Pardo, 2011), akıllı şehirlerin 3 temel aktörü bulunmaktadır. Bunlar; insan, teknoloji ve kurumlardır. Bu üç faktörün, akıllı şehri oluşturan temel bileşenler olması nedeniyle, akıllı şehirlerin işlevselliğini sürdürebilmesi adına aktörlerin bir arada uyum içerisinde çalışması gerekmektedir. Teknoloji, insan ve kurum faktörlerinin birbirine bağlı ve bir arada çalışma stratejisine dayalı olarak çalışan akıllı şehirlerde, bu 3 faktörün birbirleri içerisinde de uyumlu bir şekilde çalışabilir olması da her 6 boyutun da varlığını olumlu yönde etkileyecek ve şehre, akıllı şehir olma yolunda katkı sağlayacaktır.

Şekil 3 Akıllı Şehirlerin 3 Temel Aktörü

1.1.2.1. İnsan Faktörü

Akıllı şehirlerin odak noktası insandır. Akıllı şehirlerin temel amacı insan yaşamını daha verimli ve kolay hale getirmek olması sebebiyle diğer faktörlerden birinci derecede etkilenecek olan aktördür.

Akıllı şehirlerin getirdiği yenilikler, insanlar tarafından kabul edildiği ve kullanılabildiği derecede verimli olacaktır. Şehir her ne kadar ileri teknolojili cihazlarla donatılmış olursa olsun, insanların bu değişimi kabul ettiği kadar akıllı olacaktır.

Bununla birlikte, insanı sadece servisleri kullanacak aktöre indirgemek doğru bir yaklaşım değildir. Teknolojik altyapı tarafından sağlanacak hizmetlerin, sağladığı verilerle temel besleyicisi, zeka ve yaratıcılığıyla sistemi ileriye taşıyacak faktördür.

Veri üretimi ve işlenmesi, akıllı şehirlerin sağlayacağı servisler tarafından hayati önem taşır. Toplanacak verinin büyüklüğü ve çeşitliliği sağlanacak hizmetlerin kalitesini ve verimliliğini arttıracaktır. Verinin niceliği ve niteliğinin arttırılması bakımından, sadece şehirde kalıcı olarak ikamet edenler değil, şehirde çeşitli sebeplerle geçici olarak bulunan misafirlerin de katılımını sağlamak, izlenmesi gereken yoldur.

Akıllı şehirlerde toplanacak verinin ana kaynağının, hizmet sağlanacak aktör olan insan olacağı göz önünde bulundurulduğunda akıllı şehir gelişimi ve işlevselliğin korunması açısından insan katılımı önem taşır. Bu noktada insanlara özellikle akıllı şehir konseptinde e-platformlar üzerinden fikirlerini, becerilerini ve yaratıcılıklarını ortaya koyabilecekleri ortamlar hazırlayarak hem şehir yönetiminde söz sahibi olmaları hem de şehir gelişimine katkıda bulunmaları sağlanmalıdır.

İnsanların, teknoloji ve kurumlarla bir arada çalışabilmesi kadar insanların da birbirine bağlı ve bir arada çalışması akıllı şehir konseptine olumlu katkılar verecektir. Akıllı şehirlerde paylaşım ekonomisinin teşvik edilmesi her bir boyut için önem arz etmektedir. Eldeki kaynakların en verimli şekilde kullanılmasını amaçlayan akıllı şehirler bu yöntemle hem israfı azaltmak hem de doğaya verilen zararı minimuma indirgemeyi amaçlar. Eldeki kaynaklar paylaşıldıkça kaynaklara

olan ihtiyaç ve dolayısıyla doğaya verilen zarar da azalacaktır. Tüketici bir toplumun yerine paylaşan bir toplumun akıllı şehir gelişimine katkı sağlayacağı şüphesizdir. Geleneksel şehirlerin problemlerine yeni bir çözüm olarak doğan akıllı şehirler, paylaşım ekonomisini teşvik ederek başlıca sorunların çözüm sürecine katkı sağlayacaktır. Bu sorunlardan bazıları trafik, doğaya salınan zararlı gaz miktarı, barınma ihtiyaçlarının karşılanamaması olarak sıralanabilir. Örnek olarak e-paylaşım platformları aracılığıyla ulaşım araçlarının paylaşımlı olarak kullanılmasının yaygınlaşmasıyla trafikteki araç miktarı azalacak ve dolayısıyla bu araçlardan doğaya salınan gaz miktarı da azalacaktır. Airbnb[1] gibi platformların artmasıyla da evlerde bulunan fazla alanların verimli bir şekilde kullanımı artacak bu da hem barınma ihtiyacının verimli bir şekilde karşılanmasının yanında paylaşımcılara ek gelir olarak fayda sağlayacaktır.

Bu noktada dikkat edilmesi gereken hususlardan bir diğeri de paylaşımcı insanların yaratılmasının tek başına yeterli olmayacağı aynı zamanda akıllı şehirler faktörlerinin birbirine bağlı çalışan doğası gereği insanlara bilgi teknolojileri yeteneklerinin de kazandırılması gerektiğidir.

Özellikle üniversite ve araştırma merkezlerinin, akıllı şehirlerde yaşayacak insanların gelişimini desteklemesi, girişimciliği arttırması ve bu insanları yeni oluşacak iş alanları üzerinde yeterlilik kazandırması sağlanmalıdır. Bunların yanında özel şirketler de çalışanların eğitimini takip ederek ve yetenekli insanlara yapacakları yatırımlarla insanlara akıllı şehir vizyonu katmada katkı sağlayacaktır. (Dameri, 2017)

Güvenli akıllı şehir konseptinin uygulanabilmesi için de insan faktörü her adımda göz önünde bulundurulmalıdır. Akıllı şehirlere gerçekleştirilecek saldırılarda insan faktörü ana hedef olarak alınabileceği gibi araç olarak kullanılması da olasıdır.

[1] İnsanların evlerini kiraya verebilmesini ve diğer insanların evlerinde ücret karşılığı konaklayabilmesini sağlayan platform.

Başarılı bir şekilde gerçekleşecek bir siber saldırıdan da olumsuz olarak etkilenecek ana aktör de insan olacaktır.

1.1.2.2. Teknoloji Faktörü

Şehri "akıllı" yapan bir diğer faktör de teknoloji faktörüdür. Her bir faktörün iç içe bir uyum içerisinde çalıştığı akıllı şehirlerde teknoloji faktörünün eksikliği düşünülemez. Birçok bilimsel makalede de akıllı şehir tanımlarının ortak noktası teknolojinin insan yararına kullanımıdır. (Partridge, 2004; Harrison et al., 2010). Diğer faktörler gibi teknoloji faktörü de gerekli fakat tek başına yeterli değildir. Akıllı şehir oluşumunda bilgi teknolojileri altyapısı ve uygulamaları ön koşul olsa bile güçler birliği, kamu kuruluşları, özel sektör, eğitim kurumları ve en önemlisi insan katılımı sağlanamadığı bir oluşumdan akıllı şehir olarak bahsetmek mümkün olmayacaktır. (Lindskog 2004).

Teknoloji faktörünün şehre getirdiği fonksiyonelliklerden en önemlileri aşağıdaki gibi sıralanabilir:

- Kullanılan cihazlar aracılığıyla işlenecek verilerin toplanması
- Toplanan verilerin analiz edilmesi
- Verilerin analiz edilmesiyle çıkan sonuçlara dayalı kaynakların en optimize şekillerde kullanılmasının sağlanması
- Toplanan veriler üzerinden daha yüksek doğruluk oranı sahip tahmini analizler gerçekleştirme. (Suç işleneceğinin tahmin edilmesi vb.)
- İnsanların şehir gelişimine katkıda bulunabilecekleri e-platform hizmeti sağlanması
- Sağlanacak hizmet verimliliğinin maksimize edilmesi ve ulaşılabilirliğinin arttırılması
- Herkesin kullanımına açık veri kaynakları oluşturarak bilgi paylaşımının ve ulaşılabilirliğinin arttırılması
- Doğaya zararsız çözümler sunulması

Teknoloji faktörünün bunlar gibi birçok fonksiyonellik getirme ve bununla birlikte insan hayatını kolaylaştırma, sürdürülebilirliği ve verimliliği arttırma potansiyeline sahiptir. Fakat bir diğer yandan uygun teknolojik cihazların kullanılmaması, yanlış yapılandırmalar gibi hatalar beraberinde problemleri de getirecektir. Bu problemlerden bir tanesi yüksek maliyete rağmen verim elde edilememesidir. Verimliliği arttırmak yerine yüksek maliyetiyle birlikte şehir ekonomisine olumsuz etki edecektir.

Bir diğer problem ise cihazların yanlış yapılandırmalarıyla birlikte doğacak olan verilerin yetersiz veya gereksiz toplanması, yanlış işlenmesi sonucuyla şehri daha büyük bir kaos içerisine sokacaktır.
Üçüncü ve bu tezin asıl konusu olan problem ise güvenlik problemidir. Şehrin sahip olduğu elektronik cihazlarla birlikte, mobil cihazlarıyla şehir ağına katılacak olan insanlar da güvenlik açıklıklarıyla oluşacak olan bir siber saldırıdan doğrudan etkilenecektir. Bu saldırıların çeşitleri, kaynağı ve sonuçları tezin altıncı bölümünde ayrıntılarıyla aktarılacaktır.

Teknolojinin kullanımı konusunda gerekli önlemlerin alınması, kar-zarar ve etki analizinin iyi yapılması bunlarla birlikte güvenlik testlerinin gerçekleştirilmesi ve güvenlik açıklıklarının kapatılmasıyla birlikte şehrin akıllanmasında büyük bir rol alacaktır. Aksi durumda ise yaşanacak bir olumsuz olay ile birlikte insanların yaşamı negatif yönde etkilenecek hatta olayın büyüklüğüyle orantılı olarak şehir kaosa sürüklenecektir.

1.1.2.3. Kurum Faktörü

Kurum faktörü şehrin yönetimi olarak ifade edilmiştir. İlk bakışta her ne kadar akıllılaşmaya doğrudan etkisi yokmuş gibi görünse de akıllı şehirler için yeri vazgeçilmez olan faktörlerden birisidir. Şehrin planlanmasında, stratejilerin belirlenmesinde ve fonlama konusunda rol alır.

Yürütücü güç olan kurum faktörü, yapılacak olan yatırımlardan pozitif sonuç almakla yükümlüdür. Akıllı şehirlerin başarılı olmasından sorumlu faktör olacağı için alacağı kararlar ve yapacağı yatırımlar şehrin geleceği için kritik önem taşır. Ayrıca atacağı adımlar ve çıkaracağı yasalarla hem iş birliği ortamının hem de paylaşımcı ekonominin oluşmasında rol alacaktır. Aynı zamanda yaşanabilecek olumsuz olaylarda karşılaşılacak zararı en aza indirgemek ve kişilerin mahremiyetini korumak da bu faktörün sorumlulukları arasındadır.

İKİNCİ BÖLÜM

ÖRNEK AKILLI ŞEHİR İNCELEMESİ

2.1. ÖRNEK AKILLI ŞEHİR: KOPENHAG

İsveç merkezli EasyParkGroup şirketinin yapmış olduğu akıllı şehir endeksine göre Kopenhag şehri, değerlendirildiği 7 kategoride aldığı ortalama 8.24/10 puanla en akıllı şehir olarak değerlendirilmiştir. (EasyPark, 2017) Bu bölümde dünyanın en yaşanılabilir ve en akıllı şehirleri arasında gösterilen Danimarka'nın Kopenhag şehri, akıllı şehirlerin 6 temel boyutu referans alınarak incelenecektir.

#	CITY	COUNTRY																			RANK/ SCORE
1	Copenhagen	Denmark	9.81	8.62	8.18	6.82	7.92	9.83	8.24	6.11	9.38	8.53	7.09	5.85	9.13	8.63	7.66	4.12	9.74	8.70	9.12	8.24
2	Singapore	Singapore	7.30	6.63	4.20	10.00	2.26	8.44	7.62	7.15	10.00	5.47	7.82	5.12	8.62	8.71	7.75	6.63	7.55	8.18	9.30	7.83
3	Stockholm	Sweden	7.49	5.93	6.71	6.54	8.44	6.88	8.94	8.79	9.29	10.00	7.62	7.66	9.57	8.37	9.22	6.28	8.69	7.32	8.20	7.82
4	Zurich	Switzerland	7.80	7.75	4.98	9.83	8.62	10.00	10.00	8.70	2.07	8.10	9.03	9.02	9.74	4.69	4.38	5.59	7.55	10.00	9.00	7.75
5	Boston	United States	8.01	8.70	7.71	7.21	3.60	5.15	4.26	6.56	5.30	6.97	5.12	10.00	10.00	6.06	9.39	6.80	9.17	8.22	9.30	7.70
6	Tokyo	Japan	9.57	7.13	7.66	8.79	3.86	8.36	8.24	4.25	6.60	6.28	3.59	7.71	7.19	6.37	6.50	9.57	8.61	7.21	8.60	7.59
7	San Francisco	United States	9.05	9.05	5.08	3.43	3.60	5.15	4.26	6.38	6.23	6.59	5.44	5.67	9.91	7.91	10.00	9.05	9.17	9.01	9.10	7.55
8	Amsterdam	Netherlands	7.95	7.06	8.36	7.06	2.47	7.32	7.79	3.86	9.02	9.83	5.94	7.84	8.82	8.40	6.63	5.33	6.85	9.01	8.20	7.54
9	Geneva	Switzerland	8.06	4.98	6.11	6.97	8.62	10.00	10.00	9.13	1.80	8.36	8.59	9.14	8.96	8.11	8.79	3.94	7.55	9.80	8.10	7.53

Şekil 4 Akıllı Şehir Sıralaması

(EasyPark, 2017)

Sadece 5,7 milyon nüfusa sahip Danimarka ülkesinin, yaklaşık 1,2 milyon nüfuslu Kopenhag şehri Dünyanın en akıllı şehirleri arasında gösterilmektedir. Akıllı şehir stratejisini net bir şekilde ortaya koyan Kopenhag, planlamanın yanında yaptığı büyük çaplı yatırımlarla da bu konuda ne kadar iddialı olduğunu göstermektedir. 2014 yılında Avrupa'nın yeşil başkenti seçilen Kopenhag, 2025 yılına kadar karbondioksit salınımını sıfıra indiren ilk şehir olma hedefinde emin adımlarla ilerlemektedir.

Akıllı şehir olma yolunda 2015 yılında çıkartılan bültende temel hedef olarak yaşam kalitesini, büyümeyi ve sürdürebilirliği arttırma alınmıştır. (Teknik ve

Çevresel İdare Dairesi, 2015) Bu hedeflerin gerçekleştirilmesi için yedi kamu biriminin iş birliğiyle bir proje koordinasyon kurulu oluşturulmuş ve akıllı şehir projelerinde tek bir stratejiyle hedefe doğru yol alınmaktadır. Bu kapsamda 4 temel ilke ile projeler planlanıp hayata geçirilmektedir. Bunlar:

- Toplanan verilerin problem çözümünde kullanılması
- Yeni teknolojilerle veya bilinen teknolojilerin yeni yöntemlerle kullanılması
- Belediye veya şehir bütçesinin verimli bir şekilde kullanılması
- İnsanları ve işletmeleri sürece dahil etmek için yeni yöntemlerin kullanılmasıdır.

Şekil 5 Kopenhag Akıllı Şehir Stratejisi

(Teknik ve Çevresel İdare Dairesi, 2015)

Akıllı şehir olabilmenin en önemli şartlarından olan şehrin tüm unsurlarının katılımı ve etkileşimi ilkesi de akıllı şehir stratejisi kapsamında Kopenhag proje koordinasyon kurulu tarafından takip edilmekte, projeler üretilmekte ve hayata geçirilmektedir. Özellikle şehir sakinlerinin, paylaştıkları veriler ve geri bildirimler ile şehir gelişimine katkı sağlamaları amaçlanmaktadır. Hem Kopenhag'ın yedi kamu biriminin birbirlerine sağladıkları hem de şehir sakinlerinin geri beslemeleriyle yeni yol haritaları çizilmekte aynı zamanda mevcut sistemler de geri beslemelere dayanılarak iyileştirilmektedir. Bu kapsamda şehir sakinleri mobil uygulama ile çalışmayan veya kusurlu şehir unsurlarını raporlayabilmekte aynı

zamanda iyileştirme ve yeni proje fikirlerini de bu platform üzerinden paylaşabilmektedirler. (The Ministry of Housing, Urban and Rural Affair, 2015)

Danimarka en çok veri ve istatistik toplayan ve bu dataları sistematik şekilde derleyen ülkelerden bir tanesidir. Hem özel hem kamu sektörü bu bilgilerin toplanması ve güvenli tutulmasından sorumludur. İnsanların iş bilgilerinden kullandıkları bisiklet yollarına kadar kullanılan veriler şehri daha yaşanabilir ve daha güvenli bir yaşam merkezi haline getirebilmek adına işlenmekte ve kullanılmaktadır. Yeni projeler için şehrin bütün aktörlerinden fikirler ve geri bildirimler alındığı gibi bu kapsamdaki projeler öncesinde halka duyurulmaktadır. Böylelikle aktörler arasındaki iletişim ve halkın da katılımı sağlanmaktadır.

2.1.1. Kopenhag Akıllı Şehir Boyutlarının İncelenmesi

2.1.1.1. Akıllı Yönetişim

Akıllı şehir olma yolunda Kopenhag yönetimi de geleneksel yöntemleri değiştirerek konuya yeni bir yaklaşım getirmiştir. 7 yerel yönetimi ve 7 belediye başkanı bulunan Kopenhag şehrinde Akıllı Şehir Komitesi kurulmuştur. Bu komite üyeleri arasında belediyelerdeki önde gelen bilgi teknolojileri yöneticileri ve farklı branşlardan da birçok yönetici bulunmaktadır. Bu projeyle yönetim kademesinde de disiplinler arası projelerin entegrasyonunun daha kolay yapılması amaçlanmaktadır.

Çizilen yol haritaları ve belirlenen stratejilerle Kopenhag şehri yönetimi bu boyuta örnek bir şekilde adapte olmuştur. Belirlenen vizyon doğrultusunda çalışmaya devam etmekte, bunun denetimini ve sonuçlarını paydaşlarla paylaşmaktadır. Danimarka Hükümeti, geleceğin teknoloji, veri ve dijital platformlarda olduğu, geleceğin şehirlerinin dijital çağ ile birlikte yeniden şekilleneceğinin bilincindedir. Kopenhag başta olmak üzere bütün şehirlere yeterli teknolojik altyapının kurulması ve bunların insanların yararına kullanılmasını savunmaktadır. Ayrıca Danimarka Şehircilik Bakanı Carsten Hansen Akıllı Şehir Metodolojisi makalesinin ön sözünde şehirlerin dijitalleştiğinden emin olunması gerektiği fakat bu gelişim

sırasında şehrin asıl odak noktasının insan olduğunun unutulmaması gerektiğini vurgulamıştır. (The Ministry of Housing, Urban and Rural Affair, 2015) Şehir ne kadar dijitalleşse de şehirde yaşayan insanlar kadar akıllı olacaktır. Aynı zamanda şehrin göreceği herhangi bir negatif olaydan en çok zarar gören yine insan olacaktır.

Elektronik cihazların olduğu kadar şehrin canlı unsurlarının da iletişimine önem veren Kopenhag yönetimi uyguladığı iletişim stratejisiyle her türlü yeniliği halka ve şirketlere bildirmektedir. Şehrin her bileşenini yönetime dahil ederek yenilikçi fikirlerin önünü açmıştır. Belediye mobil uygulamasıyla şehrin her unsurundan geri besleme toplamaktadır. Yönetimin getirdiği bir diğer önemli yenilik ise kullanıcılardan ve bilgi teknolojileri cihazlarından toplanan verilerin halkın kullanımına açılmasıdır. Toplanan veriler depolanmadan önce anonimleştirildiği ve bu şekilde depolandığı açıklanmıştır.

2.1.1.2. Akıllı Ekonomi

Akıllı şehir dönüşümünün getirilerinden bir tanesi de daha güçlü bir ekonomidir. Kopenhag şehri her boyut için yaptığı yeniliklerde verim odaklı çalışarak sadece şehir yönetimine değil aynı zamanda halka da olumlu sonuçlarla dönmektedir.

Yeşil, Akıllı ve Karbon Nötr Şehir raporunda hedefleriyle gerçekleşecek enerji tasarrufu ve yenilenebilir ve daha az maliyetli enerji kaynaklarının kullanılması sonucunda her ne kadar başlangıç maliyetleri yüksek olsa da ilerleyen yıllarda maliyetini karşılayarak daha ucuz bir hizmet olarak ekonomiye pozitif bir katkıda bulunacaktır. (City of Copenhagen CPH, 2015) Bunların yanında bu enerji kaynaklarının temiz enerji kaynakları olması şehre, doğaya ve insan sağlığına verilecek zararlardan doğacak maliyetin de ortadan kalkmasını sağlayacaktır.

Kopenhag, akıllı şehir konseptiyle aynı zamanda hem yerli hem yabancı yatırımcı için daha cazip bir merkez haline getirilmek istenmektedir. Aynı zamanda start-up firmalar için büyümeye elverişli bir ortam bulunmaktadır. Şirket işletim ücretleri

bir referans noktası olarak Stockholm'den maaşlar, sosyal katkılar ve ofis kiraları bakımından %15-20 civarında daha az maliyete karşılanabilmektedir. Bunun yanında kurumlar vergisi de %22 ile Avrupa birliği ve OECD seviyelerinin altındadır. (Facts about doing business, n.d.) Daha ucuza ve daha nitelikli iş gücü bulmak daha kolaydır. İş verenler sosyal katkı payı olarak sabit yıllık 1350 Euro ödemektedir. Aynı zamanda şehir yönetimi iş sahibi olmayan insanları yetenek ve uzmanlık alanlarına göre şirketlere önermektedir.

Akıllı şehre dönüşümle birlikte açılacak birçok pozisyonun yanında şehir yönetimi yeni mezun ve staj pozisyonları açmaları konusunda şirketleri teşvik etmektedir. Yabancı çalışanlar ve yatırımcılar için de oldukça çekici bir merkez olan Kopenhag'da yabancı işçi çalıştırmak isteyen şirketler için de kolaylıklar sağlanmaktadır.

Tüm bunların yanı sıra paylaşımcı ekonominin teşvik edilmesi de henüz olgunlaşmamış olsa da planlanan projelerden bir tanesidir. Özellikle LetsGo gibi Danimarka kökenli araç paylaşım uygulamalarıyla, trafikteki araçların azaltılması ve enerji kullanımından tasarruf edilmesi planlanmaktadır. (LetsGo, n.d.)

2.1.1.3. Akıllı Ulaşım

Ulaşım imkanlarının arttırılması ve daha verimli hale getirilmesi akıllı şehir olma sürecinde önemli birer unsur olarak Kopenhag'ın akıllı şehir stratejisine dahil olmuştur.

Kopenhag şehrinde bulunan sokak ışıkları aynı zamanda kablosuz ağ erişim noktaları olarak görev almaktadır. (Copenhagen a Smart City, 2017) Bu erişim noktalarının getirdiği en büyük yenilik kullanıcıların cep telefonlarından, bisikletlerden, otobüs ve arabalardan analiz edilmek üzere veri toplamasıdır. Bu veriler ışığında şehir yollarının kullanımı daha iyi analiz edilebilmekte ve trafiğin akışı daha verimli bir şekilde yönetilebilmektedir. Bunun sonucunda şehirdeki

trafik yoğunluğu ve aynı zamanda doğaya salınan karbondioksit salınımı da belirgin bir şekilde azalmıştır.

Birbirlerine bağlı olarak çalışan bu trafik bileşenlerinin gerçek zamanlı olarak ürettiği analizler sayesinde trafiğin azalmasının yanı sıra arabaların park alanı arama sırasında kaybettiği vakit en aza indirgenmektedir. Park alanlarında bulunan sensörler ile birlikte sürücüler mobil uygulama üzerinden en yakın ve uygun park yerine bularak zaman tasarrufu yapmaktadırlar. Bu uygulama sonucunda şehrin kilit noktalarında trafik miktarının azaldığı kaydedilmiştir.

Toplu taşıma biletleri Mobilbiletter adlı uygulama üzerinden alınabilmektedir. Bu uygulama telefondan alınan GPS sinyalleriyle ve ulaşılacak nokta bilgisiyle kullanıcıya en kısa ve en hesaplı rotayı önermektedir.

Bunların yanında gelişmiş bisiklet yolu ağıyla bisiklet dostu olan bir şehir olan Kopenhag'da insanların yarısından fazlası iş yeri veya öğretim kurumlarına erişimi sırasında bisiklet kullanmaktadır. Bu da hem enerji tüketimini azaltarak ekonomiye fayda sağlamakta hem de zararlı gaz salınımını azaltarak doğaya verilen zararı azaltmaktadır. (LetsGo, n.d.)

2.1.1.4. Akıllı Yaşam

Akıllı şehrin öncelikli hedefi, şehri daha yaşanılır bir yer haline getirerek insanların hayatını kolaylaştırmaktır. Kopenhag'ın akıllı şehir stratejisi de bu yönde gelişmiştir. Şehrin tüm unsurlarıyla entegre olarak çalışan teknolojik altyapıyla şehir yaşantısının daha sağlıklı, verimli, sürdürülebilir ve kolay olması amaçlanmaktadır.

Kopenhag şehrinde öncelikle şehrin öncelikli olarak kilit noktaları olmak üzere kablosuz ağ erişim noktalarıyla donatılmıştır. Özellikle şehre misafir insanlar olmak üzere tüm insanlar internet erişimiyle sunulan hizmetlerden

faydalanabileceklerdir. Erişilebilir açık veri kaynaklarıyla ihtiyaç duyulan verilerden yararlanabileceklerdir.

Sensör ağlarıyla optimize edilen yolları kullanan insanlar, ulaşmak istedikleri noktalara trafikte bekleme süreleri en aza indirgenerek yolculuk etmektedirler. Bunun yanında park alanlardaki sensörler de park yeri arama süresini azaltarak insanların zaman tasarrufu yapmalarını sağlamaktadırlar. Belediyenin mobil uygulaması üzerinden GPS sinyalleriyle mevcut konum ve hedef konum girdileri kullanılarak olabilecek en kısa yolculuk süreli ve en hesaplı yolculuk rotası kullanıcılara sunulmaktadır.

Gelişmiş bisiklet yolu ağıyla bisiklet kullanım oranının çok yüksek olduğu şehirde her noktanın bisikletle ulaşılabilir olması planlanmaktadır. Böylelikle insanlar hem daha aktif hem de zararlı gaz salınımından azami şekilde etkilenerek daha sağlıklı bir yaşam sürmektedirler.

Akıllı atık projesiyle dolan atık kutuları sinyaller göndermekte ve ilgili ekipler duruma göre aksiyon almaktadırlar. Bu sensörler aynı zamanda zararlı atık şüphesinde de alarm üretmektedir ve tüm canlıların sağlığının korunması amaçlanmaktadır.

Bunlarla birlikte şehirde akıllı su savunması sistemi bulunmaktadır. Olası bir sel durumunda sensörler alarm üretmekte ve uygun aksiyonun alınması sağlanmaktadır.

Kullanılmakta olan sensörlerin bir diğer kullanım alanı ise şehir sakinlerinin güvenliğinin sağlanmasıdır. İnsanların sahip oldukları varlıklara yerleştirilen RFID etiketleriyle özellikle çalıntı olaylarının büyük ölçekte önüne geçilmesi başarılmış ve hırsızlık oranları belirgin ölçüde azaltılmıştır. (Teknik ve Çevresel İdare Dairesi, 2015) Bu cihazların yanında şehirde bulunan kameralar da olası suç durumlarının

önceden belirlenmesi ve müdahale edilmesi veya oluşan suç durumlarında faillerin yakalanması hususunda önem taşımaktadırlar.

Akıllı şehirlerin teknoloji altyapılarının doğru kullanılması durumunda hayat kalitesini arttırması beklenmektedir. Özellikle siber saldırılarla cihazların kontrolünün kaybedilmesi gibi aksi durumda ise yaşanıla bilirliğin düşmesi hatta şehirde yaşamın durma noktasına kadar gelmesi kaçınılmaz olacaktır.

2.1.1.5. Akıllı İnsan

Şehrin karar alma mekanizmasına dahil olan şehir sakinlerinin yetki ve yetenekleri önemli bir konudur. Kopenhag'ın büyüme politikasında Kopenhag şehri insanlarının öğrenim seviyesinin yükseltilmesinin öneminden bahsedilmektedir. (City of Copenhagen, 2015) Akıllı şehir imkanlarıyla açılan yeni meslek alanlarını dolduracak insan potansiyelinin sağlanması da insanlara iyi ve yenilikçi bir eğitim olanağı sağlayarak gerçekleşecektir. Özellikle disiplinler arası projeler yürüten lisans ve ön lisans programlarıyla okullar hem gençler için daha cazip kılınmakta hem de akıllı hale gelen şehir için gerekli insan gücünü üreten merkezler haline gelmektedir. Kopenhag şehrindeki insanların tümünün en az ön lisans seviyesinde öğrenim derecesine sahip olması amaçlanmaktadır.

Okullardan kazandıkları bilgi birikimi ve yetkinliklerine göre öğrenciler, uygun iş alanlarına yönlendirilmektedir. İş sahibi olmayan fakat uygun yeteneklere ve yeterliliğe sahip mezunlar şirketlere önerilmektedir. Bunun yanında küçük ve orta ölçekteki şirketler ve mezun ya da mezun olmaya yakın öğrenciler kendilerine en uygun akademisyenle eşleştirilmektedir. Bu sayede şirketlere büyümelerinde yardımcı olunmakta, öğrencilere ise kendileri için en doğru kararı almalarında danışmanlık yapılmaktadır. (City of Copenhagen, 2015)

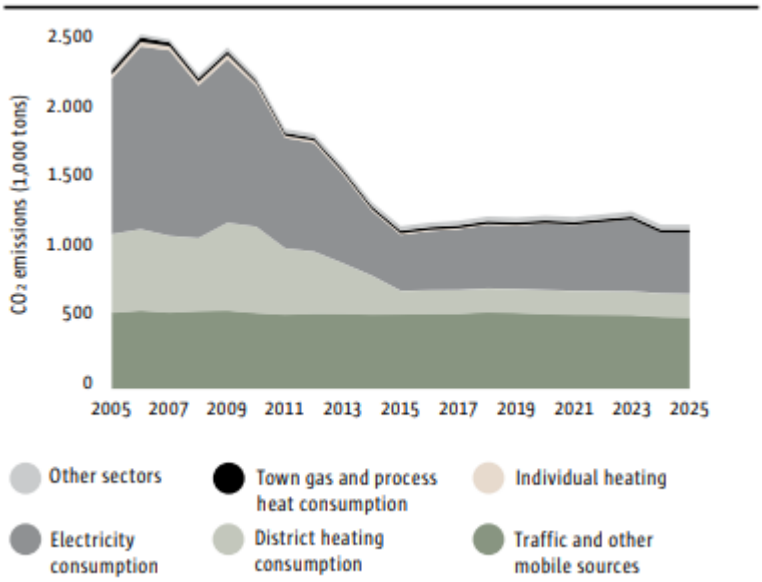
Şehrin temel yapıtaşı olan insanların ekonomiye katkı sağlayacak bireyler olarak yetiştirilmesi de eğitim ve öğretim hayatları süresi içerisinde verilmesi

planlanmaktadır. Her seviyedeki eğitim kurumlarında öğrencilerin daha yenilikçi, girişken ve yaratıcı bireyler olarak hayata atılması amaçlanmaktadır. Aynı zamanda üniversiteler ve şirketler arasında iş birliğinin arttırılmasıyla öğrencilerin iş hayatına daha erken adapta olması sağlanmaktadır.

Üniversitelerin yanında şehir tarafından verilen servislerle de insanların daha üretken ve şehir gelişimine faydalı olmaları sağlanmaktadır. Mobil ve web uygulamalar aracılığıyla insanlar bilgilendirilmekte ve sağlayacakları verilerle katılımlarının arttırılması amaçlanmaktadır. Bu uygulamalar üzerinden insanlar hem yeni fikirlerle hem de mevcut veri havuzuna katkıda bulunarak şehrin akıllılaşmasına yardımcı olmaktadırlar. Bunlara ek olarak siyasal seçimlere kadar çok çeşit verinin bulunduğu şehrin açık veri kaynaklarından yararlanabilmektedirler.

2.1.1.6. Akıllı Çevre

Gerek gerçekçi stratejisi gerek hayata geçirdiği ve planladığı projeler ile Kopenhag doğaya en duyarlı şehirlerden biri olmuştur. Akıllı şehir stratejisiyle de en önemli hedefin 2025 yılına kadar zararlı gaz salınımını sıfıra indirgemek olduğunu dile getiren Kopenhag belediye başkanı Frank Jensen, sadece yönetimin değil aynı zamanda yerel halkında yenilenebilir enerji kaynaklarına yatırımlarda bulunduğunun altını çizmektedir. Kopenhag şehri, 2025 Yeşil, Akıllı ve Karbon Nötr Şehir raporuyla ve yapılan yatırımlarla bu konudaki kararlılığını ortaya koymuştur. Aynı zamanda bu süreçte karşılaşılacak zorluklar, maliyetler, getiriler ve çözüm önerileri de bu rapor içerisinde detaylı bir şekilde kamuoyuna sunulmuştur. (City of Copenhagen CPH, 2015)



Şekil 6 Mevcut durumda 2025' e kadar planlanan Karbon Salınım Miktarları

(City of Copenhagen CPH, 2015)

Raporda hedef ulaşılması için kilit rol oynayan dört faktörden bahsedilmektedir:

- Yeşil enerji üretimi
- Enerji harcamalarının azaltılması
- Yeşil taşımacılık
- Şehir yönetimi girişimleri

Bu faktörler üzerinde yoğunlaşan rapor, enerji üretimi konusunda yenilenebilir enerji kaynaklarından faydalanılmasını, fosil yakıt yerine farklı tür enerji kaynaklarına geçilmesi aynı zamanda bisiklet gibi insan gücüyle çalışan araçların yaygınlaştırılmasını hedeflemekte ve şehir yönetiminin denetlemeleri yapacağını ve altyapı için gerekli harcamaların yapılarak hedefe ulaşılacağını teyit etmektedir. Yapılan bu çalışmalar sadece çevre ve iklim için yararlı değildir. Bu yatırımlarla aynı zamanda şehrin yaşana bilirliği önemli derecede artmaktadır. Bunun bilincinde olan Kopenhag şehrinin sakinleri, özel şirket ve kamu birimleri de yeşil enerji kaynaklarına yatırımlar yapmakta daha verimli enerji tüketen ürünleri tercih etmektedirler.

Binaların inşası sırasında da yeşil dostu binalar inşa edilmesi zorunlu kılınmaktadır. Bu şekilde inşa edilen binalar enerjiyi daha verimli kullanmaktadırlar. Bu proje aynı zamanda mevcut binalar için de uygulanabilmektedir. Bu projeler şehre yayılmadan önce şehir yönetiminin binaları üzerinde denenmekte ve sonrasında diğer binalar için uygulanmaktadır.

Enerji üretimi için ana kaynak olarak rüzgar, jeotermal, biyo-yakıtlar ve güneş enerjisi tercih ve teşvik edilmektedir. Fakat altyapının yetersizliği ve bu altyapıların kurulması ve yeni enerji kaynaklarına geçiş sürecinde doğaya verilecek zararlar büyük bir engel olarak ortaya çıkmaktadır. Tamamen yenilenebilir enerjiye geçiş için gerekli altyapıların kurulması ve uygulanmaya başlamasının 2035 yılına kadar sürmesi beklenmektedir.

Tüm bu yatırımlar doğaya ve insan yaşamına katkı sağladığı gibi uzun vadede ekonomik olarak hem şehri hem de ülkeyi pozitif anlamda etkilemesi ve yatırımları kısa sürede nötrlemesi beklenmektedir.

Yeşil bir gelecek için çalışan Kopenhag şehrinin tüm aktörleri bu çalışmalar ve planlar sonucunda 2014 yılında Avrupa'nın Yeşil Başkenti seçilmiştir.

2.1.2. Kopenhag Akıllı Şehir Uygulaması Getirileri

Akıllı şehir yatırımlarını ciddi boyutlara taşıyan Kopenhag şehri, bu yatırımların karşılığını almaktadır. Ana hedef olarak 2025 yılı itibariyle karbon salınımının nötr hale getirilmesi belirlenmiş ve bu yolda da ciddi bir yol kat edilmiştir.
2014 yılında Avrupa'nın yeşil başkenti ve En Bağlantılı Şehir seçilen Kopenhag şehri (Teknik ve Çevresel İdare Dairesi, 2015), 2008, 2013 ve 2014 yıllarında en yaşanılabilir şehir seçilmiştir. (Most Liveable City, n.d.)
Kopenhag Akıllı Şehir Raporu 2015 'te yayınlanan akıllı şehir dönüşümünün şehre kattıkları aşağıda listelenmiştir:

- %11-32 oranında trafik optimizasyonu
- Arabada geçirilen zamandan yılda 2,4 milyon saat tasarrufu
- Araba yolculuklarında 30,7 milyon kilometrelik azalma ile 1,7 milyon litre yakıt tasarrufu
- Su tüketiminde 5,5 milyon metreküp azalma
- Karbondioksit salınımında 180.000 azalma
- Bisiklet hırsızlığında %50 azalma
- Turizm gelirlerinde %1'lik artış
- 104 milyon € değerinde iş olanağı sağlanması (Teknik ve Çevresel İdare Dairesi, 2015)

Kopenhag şehrinde olduğu gibi akıllı şehir stratejisini net bir şekilde belirleyen ve uygulayan şehirlerin başarılı olması kaçınılmazdır. Bu konseptte özellikle bilgi teknolojileri alt yapılarının uygun yapılandırılması ve güvenlik eksikliklerinin giderilmesi yukarıda listelenen başarılı sonuçlara ulaşılabilmesi için büyük önem taşır.

ÜÇÜNCÜ BÖLÜM

AKILLI ŞEHİR KONSEPTİNDE YARARLANILAN TEKNOLOJİLER VE ÖRNEK KULLANIM ALANLARI

3.1. AKILLI ŞEHİRLERDE TEKNOLOJİ

Merkezine insan hayatını alan ve hayat kalitesini arttırmayı amaçlayan akıllı şehirleri, geleneksel şehir anlayışından ayıran en önemli unsurlardan biri şüphesiz ki kullanılan teknolojilerdir. Her alanda olduğu gibi şehirciliğin de günümüz teknolojisini takip eden, kullanılabileceği ve verim sağlayabileceği teknolojileri şehir bünyesine katan bir anlayışla yürütülmesi gerekmektedir. Günümüz dünyasında bu durum şehrin hem yaşanıla bilirliği hem de sürdürebilirliği açısından kaçınılmaz bir hal almıştır. Teknoloji kullanımıyla insanların ihtiyaçlarını daha verimli karşılayarak hayat kalitesi arttırılmakla kalınmayacak, aynı zamanda bu ihtiyaçlar da teknoloji yardımıyla tespit edilebilecektir. Bu tür girişimlerle özel kuruluşlar ve kamu kuruluşları hizmet verdikleri kitleyi daha iyi anlayacak konuma geleceklerdir.

Kablosuz bir şekilde birbirleriyle haberleşebilen bu cihazlar birbirleri arasında bir ağ oluşturmaktadırlar. İletişim halinde olan cihazlardan oluşan bu ağ izleme, veri toplama, toplanan verinin kıymetlendirilmesi ve yorumlanarak çözüm üretilmesi gibi görevleri minimum insan müdahalesiyle gerçekleştirebilmektedir.

Bu bölümde akıllı şehirlerde yaygın olarak kullanılan teknolojiler ve örnek kullanım alanları, yedi ana başlık altında incelenecektir: mobil cihazlar ve dijital platformlar, büyük veri ve açık veri, nesnelerin interneti, 3 boyutlu baskı, sosyal etkileşimli robotlar, insansız hava araçları.

Şekil 7 Akıllı Şehir Teknolojileri

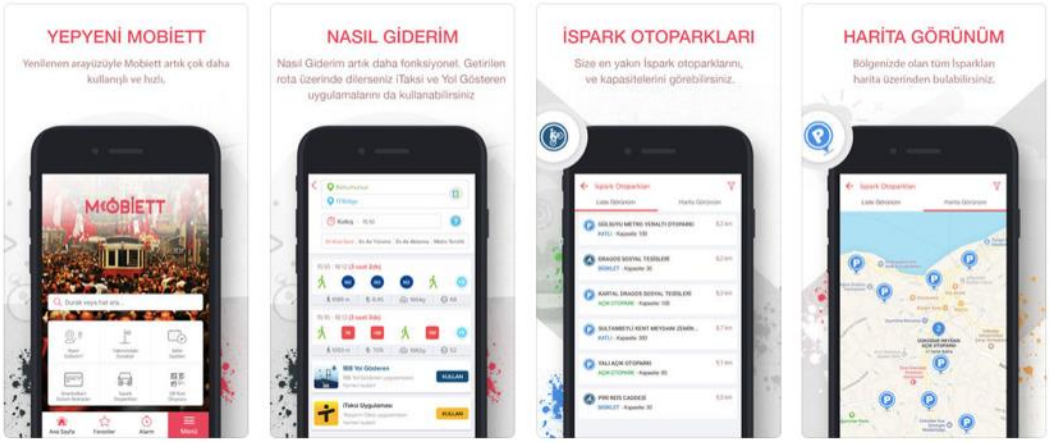
3.1.1. Mobil Cihazlar ve Dijital Platformlar

Özellikle geçtiğimiz on yıldan itibaren mobil yani taşınabilir cihazlar, insan hayatını ciddi boyutlarda değiştirmeye başlamıştır. Her an ve her yerde kullanıcıya kablosuz internet bağlantısı ve GPS sinyali imkanı veren bu cihazlar bilgi çağının başlamasına neden olan unsurlardır. Mobil cihaz teknolojisi hayatımızda her alana girmiş, giyilebilir aksesuarlarımız dahi dış dünyayla her an bağlantılı durumdadır. Günümüzde veriye ulaşmak hiç olmadığı kadar kolaylaşmıştır. İnsanlar fiziksel olarak bir yerde bulunmaya veya fiziksel bir bilgi kaynağına sahip olmaya gerek olmadan her an veriye ulaşabilir bir pozisyona gelmiştir. İnsanlar da aynı şekilde günün her saati ulaşılabilir durumdadırlar ve hayatın her alanındaki değişikliklerden eş zamanlı olarak haberdar olabilmektedirler.

Mobil cihazları özel kılan en önemli faktörlerden bir tanesi de sayısı her saniye artan mobil uygulamalardır. Hizmet veren tarafın kullanıcıya erişim noktası olan mobil uygulamalar ulaşımdan, eğlenceye, sağlığa, bankacılıktan, güvenliğe birçok hizmetin kullanıcıyla buluşturulduğu noktadır. Şekil 3-4-5'de İstanbul'da kullanılmakta olan iTaksi, Mobiett ve IBB CepTrafik gibi uygulamlar söz konusu ulaşım ile ilgili mobil uygulamalara örnek olarak verilmiştir.

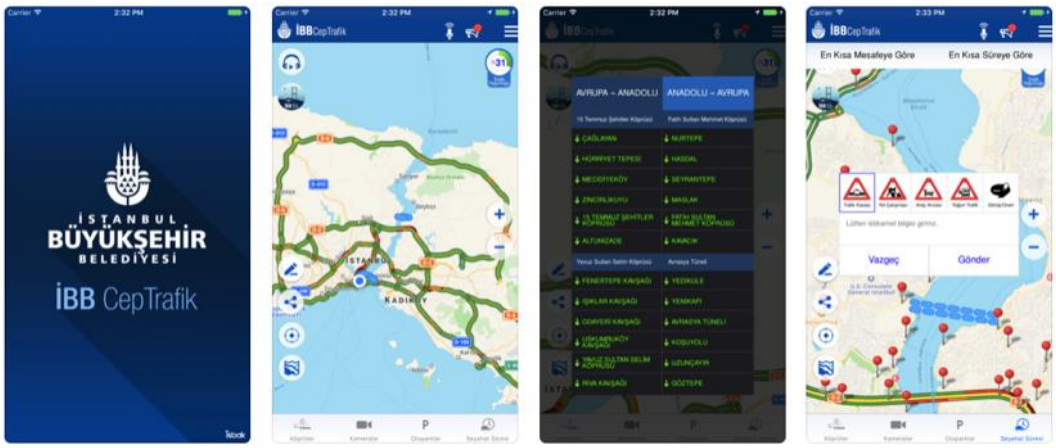
Şekil 8 iTaksi Uygulaması

(Istanbul Büyükşehir Belediye Başkanlığı, 2018)



Şekil 9 Mobiett Uygulaması

(İETT İşletmeleri Genel Müdürlüğü, 2018)



Şekil 10 IBB CepTrafik Uygulaması

(Istanbul Büyükşehir Belediye Başkanlığı, 2018)

Şekil 11 Evreka Akıllı Atık Toplama Sistemi

(Evreka, 2018)

Her saniye insanın yanında olan bu cihazlar, kullanıcılardan gelecek bilginin en önemli kaynağıdır. GPS sinyalleriyle konum bilgisi ve bunun gibi depoladıkları kullanıcıya özel birçok veri, hizmet sağlayıcılar tarafından analiz edilerek kullanıcıya özelleştirilmiş hizmet olarak geri dönmektedir.

Mobil uygulamalar aracılığıyla hizmet sunan dijital platformlar, özel kurumlar ve kamu kuruluşları için yeni iş modelleri oluşturmakta, sosyal, ekonomik ve aynı zamanda kültürel anlamda insan hayatında etkili bir rol oynamaktadır. Hizmet sağlayıcıları kullanıcılarla veya her iki aktörü kendi aralarında bir araya getiren

dijital yapılardır. Bu yapılar aracılığıyla insanlar görüş ve fikirlerini diğer kullanıcılarla veya hizmet sağlayıcılarla ve yöneticilerle paylaşabilmekte bunun sonucunda hizmet sağlayıcılar için hizmet kalitesini arttırma fırsatı doğmaktadır.

Temeli her bir aktörün birbiriyle bağlantılı çalışması olan akıllı şehirler için de mobil cihazlar, şehir hizmetlerinin kullanıcıya ulaştırıldığı kanallardan bir tanesidir. Bu cihazlarla şehrin kablosuz ağ erişim noktalarına bağlanan kullanıcılar, kablosuz ağa dahil olarak şehrin teknolojik altyapısının canlı birer parçası olacaklardır. Böylelikle mobil cihazlar akıllı şehrin sunduğu akıllı çözümlere erişilebilecek bir kanal görevi görecektir.

Dünyanın akıllılaşan şehirlerinde mobil cihazlar, bu cihazlara yüklenecek çeşitli mobil uygulamalar ile birlikte çok geniş kullanım alanlarına sahiptir. Hayatı kolaylaştıracak servislerin yanında kurulacak dijital platformlarla halkın, şehrin diğer aktörleriyle etkileşimi de mümkün hale gelmektedir. Bu platformlar üzerinden kullanıcılar yeniliklerden ve projelerden haberdar olabilir, geri besleme ve fikirleriyle yönetimde söz sahibi olabilirler. İnsanları bir araya getirerek paylaşım ekonomisi kavramını ortaya çıkartan AirBnb, Couchsurfing[2], Uber[3] gibi platformlar daha hesaplı hizmetler sunmakta ve eldeki kaynakların en verimli şekilde kullanılmasına yardımcı olmaktadır.

Mobil cihazlara yüklenebilecek uygulamalar ve erilebilecek dijital platformlar incelendiğinde belediyeler tarafından verilen ulaşım hizmetlerinin mobil uygulamalar ile birlikte daha verimli ve akıllı bir şekilde sağlandığı görülmektedir.

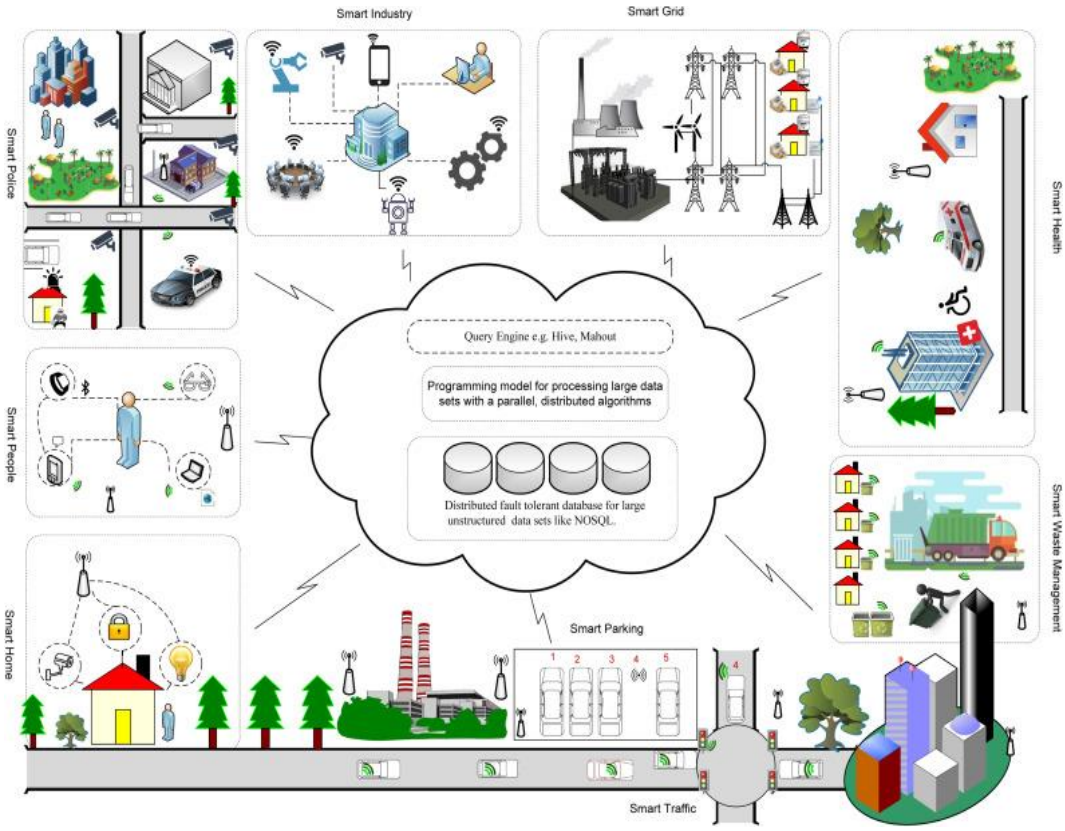
3.1.2. Büyük Veri ve Açık Veri

Özellikle bilgisayarların hayatımıza girdiği andan itibaren tüm dünya üzerinde toplanan veri miktarı ciddi boyutlara ulaşmıştır. İlerleyen teknolojiyle ve geliştirilen algoritmalarla birlikte çok büyük boyutlardaki verilerden daha anlamlı

[2] İnsanların evlerindeki ekstra kanepe ve yatakları diğer insanların kullanımına açtığı platform.
[3] İnsanların araçlarıyla yolcu taşımacılığı yapmalarına olanak sağlayan platform.

çıkarımlar yapılmaya başlanmıştır. Son yıllarda adı sıkça duyulan büyük veri, Microsoft tarafından şu şekilde tanımlanmıştır: "Büyük veri; ciddi işlemci gücü, makine öğrenimi ve yapay zeka algoritmalarının ciddi anlamda büyük boyutlardaki ve çoğu zaman çok karmaşık bilgi kümelerine uygulanma sürecidir." (Microsoft, 2013)

Çoğalan kent nüfusu ile birlikte şehrin fiziksel altyapısı ile sunulan hizmet yetersiz kalmaktadır. Şehrin dijital altyapısı ile birlikte toplanacak büyük miktardaki verinin işlenerek akıllı çözümler sunulması gerekliliği ortaya çıkmıştır. Büyük veri, akıllı şehirler için, RFID etiketleri, sensörler ve izleme cihazları gibi cihazlardan toplanacak veriden faydalı iç görüler çıkartılmasına olanak sağlamakta ve akıllı şehirlere geleneksel şehirlerden ayırt edici bir unsur olarak karşımıza çıkmaktadır.



Şekil 12 Akıllı Şehirlerde Büyük Veri Kullanım Alanları

(Hashem, et al., 2016)

Toplanan veri üzerinde yapılan analizler sonucunda ulaşım, sağlık, enerji, güvenlik gibi pek çok alanda şehir halkına akıllı çözümler sunulabilmektedir.

Büyük verinin şehre katacağı üç temel fayda vardır (Nuaimi, et. Al., 2015):

- Kaynakların verimli kullanılması
- Hayat kalitesinde artış
- İleri seviyede açıklık ve şeffaflık

Sürekli bir şekilde izlenen ve kayıt altına alınan kaynak kullanımında, verimsiz kullanımın tespiti daha kolay yapılabilmekte ve kaynak israfının önüne geçilebilmektedir. Bunun yanında daha verimli şekilde dağıtılacak kaynaklarla harcanacak enerji ve doğaya verilecek zarar en aza indirgenebilecektir.

Daha verimli, ihtiyaca uygun ve doğaya saygılı çözümlerle hayat kalitesinde artış gözlemlenecektir. Zaman ve kaynaklardan edilen tasarrufla insanlar daha iyi bir yaşam sürecektir.

Toplanan ve analiz edilen verilerin açık bir şekilde sunulması akıllı şehir yönetiminin şeffaflığını arttıracak, karar alımını kolaylaştıracak, paylaşımın teşvik edilmesiyle daha farklı ve verimli hizmet alanları ortaya çıkacaktır. Bu fikir açık veri kavramı olarak karşımıza çıkmaktadır.

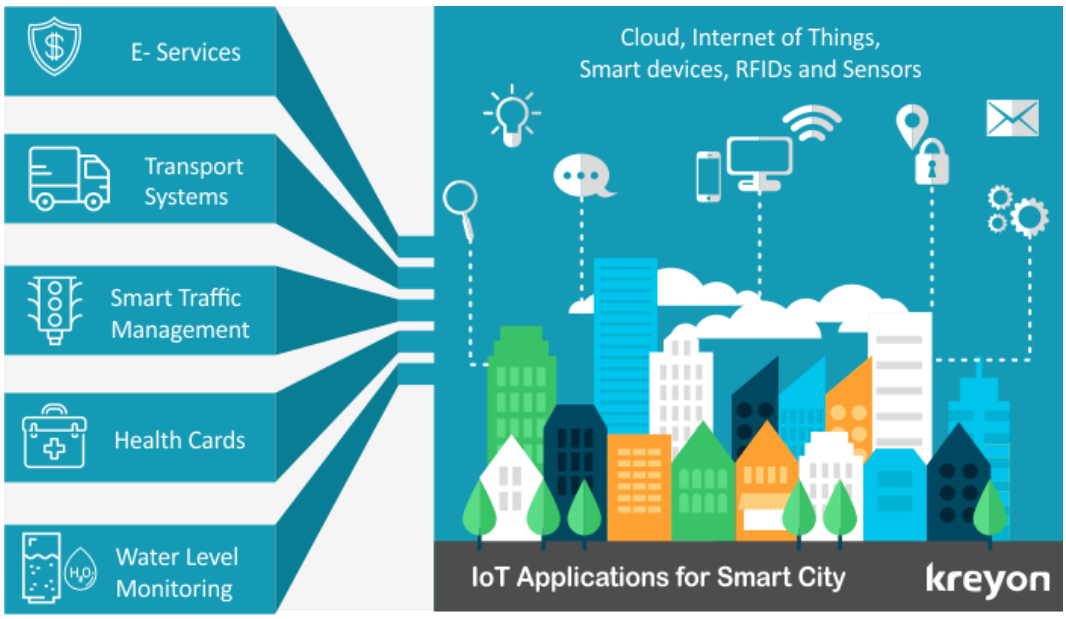
Açık veri temel olarak herkes tarafından serbest bir şekilde kullanılabilen, tekrar kullanılabilen ve dağıtılabilen veri olarak tanımlanmıştır. (Open Knowledge Foundation, 2012) Verilerin açık veri olarak değerlendirilmesiyle, akıllı şehirlerde de amaçlanan katılım artacak, disiplinlerin birbirleriyle bağlantılı olarak çalışması kolaylaşacaktır. Aynı zamanda yönetimler tarafından seçim verileri gibi verilerin insanların erişimine açılmasıyla yönetimdeki şeffaflık artacaktır.

3.1.3. Nesnelerin İnterneti

Nesnelerin interneti konsepti, etrafımızda gördüğümüz her türlü cihaza algılama, hissetme, ağ oluşturma ve veri işleme yetenekleri kazandırılarak birbirleriyle ve

diğer servislerle internet üzerinden haberleşerek yeni kullanılabilir servisler oluşturulmasıdır. (Nuaimi et al., 2014) İnternet teknolojileri, sensör ağları ve RFID gibi teknolojilerin her geçen gün daha çok yol kat etmesiyle, çevremizdeki nesneler birbirleriyle iletişim ve işlem kabiliyeti kazanmıştır. Böylelikle nesnelerin interneti konsepti hayatımızın birçok alanına girmiş ve hayatımızı kolaylaştıran hizmetlerde kullanılmaya başlanmıştır.

Nesnelerin interneti konsepti, şehirlerde sunulan akıllı hizmetlerin temelini oluşturmaktadır. Şehrin dijital altyapısındaki en önemli unsurlardan biri, birbirleriyle iletişim halinde olan cihazlardır.



Şekil 13 Akıllı Şehir ve IoT Uygulamaları

(Kreyon, 2016)

Akıllı şehirlerde birçok servisin kullanım amacı yaşayanları için daha kaliteli bir yaşam sunmaktır. Bu servislerde nesnelerin interneti konsepti kullanılarak gerekli veri toplanmaktadır. Örnek olarak akıllı trafik servisiyle kullanıcılara en verimli güzergah bilgisini sunacak bir şehirde, trafikteki tüm araçlar, internete bağlı bir nesne olarak düşünülebilir. Bu nesneler konum, mevcut yolculuk süresi, trafik yoğunluğu gibi bilgiler üreterek birbirlerine iletmektedir. Böylelikle toplanan verilerle diğer kullanıcılara daha verimli bir güzergah sunulmaktadır. Bu çözümle

birlikte şehir trafiğinde optimizasyon sağlanarak insanların trafikte bekleme süresi azaltılabilir.

Bir diğer kullanım örneği olarak Amsterdam akıllı şehir lambaları gösterilebilir. Amsterdam şehrinde şehir ışıklarında bulunan sensörler ile birlikte çevredeki aydınlık seviyesine göre ışığın parlaklığı ayarlanmakta, trafik durumu, otopark alanı gibi bilgiler kullanıcılara aktarılmaktadır.

Enerji kaynaklarından en verimli şekilde yararlanmayı hedefleyen akıllı şehirlere, nesnelerin interneti konseptiyle gelen bir diğer yenilik ise akıllı şebekelerdir. Birbirleriyle haberleşen ve sensör özellikleri bulunan nesnelerin topladığı verilerle, kullanıcılara daha verimli enerji hizmeti verilecektir.

Nesnelerin interneti konseptinin şehirlere uygulanmasıyla üretilebilecek servis olanakları yukarıdaki örneklerle sınırlamak doğru olmayacaktır. Toplanacak verinin çeşidi ve veri üzerinde yapılacak analizin kalitesi arttıkça, verilebilecek servis çeşitliliği de artacaktır.

3.1.4. 3 Boyutlu Baskı

3 boyutlu baskı, bir diğer tabirle eklemeli üretim, dijital verinin 3 boyutlu nesnelere dönüştürülmesidir. 1989-2014 yılları arasında hem Avrupa'da hem Amerika'da üretim verimliliğinde ciddi anlamda düşüş yaşanmıştır. (Scott, 2014) Bunun sonucu olarak toplu üretim konusunda verimliliği arttıracağı düşünülen 3 boyutlu baskı teknolojilerine özellikle Avrupa'da ve Çin'de büyük yatırımlar yapılmaya başlanmıştır. Dönemin Amerikan Başkanı Barrack Obama' da bu yarışta üretimin arttırılması için 3 boyutlu baskı stratejisinin önemini vurgulamıştır. (Schniederjans, 2017)

3 boyutlu baskı teknolojisinin verimliliği arttırmanın öneminin sıkça vurgulandığı akıllı şehir stratejilerinde de yer almaya başladığı görülmektedir. Bu teknolojiyle

birlikte insanlara barınma ihtiyaçlarının karşılanması daha kolay, verimli ve hızlı bir şekilde karşılanabilmektedir. Dünya'nın ilk 3 boyutlu baskıdan evini Çin'de inşa eden WinSun şirketi, 24 saat içerisinde 10 ev inşa edebileceğini öne sürmektedir. (Starr, 2015)

3 boyutlu baskı cihazlarının geri dönüşüm materyallerini de verimli bir şekilde kullanabilmektedir. Eskiyen veya kullanılmayacak durumdaki evlerin, eşyaların ve şehre ait her türlü objenin 3 boyutlu baskıyla yeniden üretilmesi insanların yaşam kalitesini arttırırken, kullanılmayan materyallerin de geri dönüşümüne katkıda bulunacaktır. İlerleyen yıllarda, gelişen teknolojiyle birlikte, bütün bir şehrin 3 boyutlu baskı ile üretilebileceği öngörülmektedir. Bu doğrultuda en büyük atılım Dubai şehrinde yapılmıştır. Yeni regülasyonlarla birlikte Dubai şehrindeki yapıların en az %25 'inin 3 boyutlu baskı çıktısı olması hedeflenmektedir. (Pyzyk, 2018)

3.1.5. Sosyal Etkileşimli Robotlar

Yapay zeka ve makine öğrenimi gibi teknolojilerin robot teknolojisi ile entegrasyonuyla, sosyal etkileşimli robotlar hayatımıza girmiştir. Bu robotları, geleneksel endüstriyel robotlardan ayıran değişime adaptasyon ve öğrenme gibi özellikleri bulunmaktadır. Eğitim, sağlık, ev işleri gibi birçok alanda insanların yaptığı işleri daha az maliyetle ve daha az hatayla yapan robotlar, akıllı şehirlerin de değişmez parçaları haline gelecektir. Özellikle Avrupa'da nüfusun yaş ortalamasının her geçen yıl artmasıyla, sosyal etkileşimli robotların da şehirlerde daha fazla rol alması beklenmektedir. (Flandorfer, 2012)

Hizmet sektörünün daha verimli sağlanmasının yanında, şehrin genel akışı içerisine de robotların hızlı bir şekilde entegre olması kaçınılmazdır. Şehri sürekli izleyecek olan robotların fark ettiği acil durumlarda görevlileri uyarması, şehrin temizliği, yollardaki bozulmaların bildirilmesi ve bunların yanında yanan binalardaki insanları kurtarma, büyük uzunluklardaki binaların temizlenmesi ve bakımı gibi

birçok alanda robotların görev aldığını göreceğiz. (Torras, 2016) Robotların şehirlere sağlayacağı katkılar yanında, özellikle birçok alanda insanların yerine geçerek iş alanlarını daraltmaları ve etik sorunlar da detaylı bir şekilde incelenmelidir.

3.1.6. İnsansız Araçlar

Öncelikle askeri amaçlı olarak kullanılmaya başlanan insansız araçları, günümüzde birçok sivil alanda da yaygın olarak kullanılmaya başlanmıştır. İnsanlar yaşayabileceği, çalışıp katkı verebileceği sürdürülebilir bir alan yaratmayı hedefleyen akıllı şehirlerde, insansız hava araçlarından faydalanılabilecek birçok alan bulunmaktadır. Bunlardan başlıcaları:

- Ölçüm için gerekli ekipmanlarla donatılarak coğrafi ölçümler yapma ve veri üretimi,
- Şehri yukarıdan veya içeriden izleyerek güvenliğin ihlal edildiği durumları tespit ederek yetkilileri bilgilendirme
- Trafik durumu hakkında veri sağlama ve trafik kuralları ihlalinin tespit edilmesi
- Tarımda gübreleme, sulama gibi birçok alanda faaliyet gösterme
- Doğal afet durumlarında arama kurtarma çalışmalarına katılma
- Çeşitli ürünlerin taşımacılığı

Yukarıda listelenen alanlar gibi çok alanda şehir hayatını daha sürdürülebilir kılmak amacıyla insansız araçlardan faydalanılabilir. İnsansız hava araçlarının kullanımı için gerekli altyapılar sağlandığında bu araçlar akıllı şehir yapılanmalarında önemli bir rol oynayacaktır. (Mohammed et al., 2014)

DÖRDÜNCÜ BÖLÜM

SİBER DÜNYA VE SİBER GÜVENLİK

4.1. SİBER UZAY

İnternet, dünya üzerinde internet protokol setini (TCP/IP) destekleyen cihazları ve ağları birbirlerine bağlayan, insanların ve bağlı cihazların birbirleriyle bilgi paylaşımı yapabildikleri ve haberleşebildikleri ağdır. Günümüzde internet, yarı iletken içeren bütün cihazları birbirine bağlayabilmektedir. Nesnelerin interneti konseptinin temel altyapısını oluşturur.

Siber uzay terimi ilk kez William Gibson'ın *"Neuromancer"* adlı romanında ortaya çıkarak yaygınlık kazanmaya başlamıştır. Bu kitapta Gibson siber uzayı, insanlar tarafından üretilen ve kullanılan saf bilginin bilgisayarlar ve bilgisayar kümeleri arasında hareket ettiği üç boyutlu bir uzay olarak tanımlamıştır. (Deibert, & Rohozinski, 2010) Siber uzay, literatürde resmi bir tanımı olmamasıyla birlikte, bilgisayarlardan, okuma, işleme, depolama, yazma, haberleşme gibi yetenekleri bulunan bilgi işlem cihazlarıyla, bu cihazları kullanan insanlar ve bu insan ve cihazların ürettiği veriden oluşan sanal bir ortamdır. Siber uzay üzerinde bu bileşenler birbirleriyle bağlantılı olarak veri paylaşımında bulunmakta, servis almakta ve sağlamaktadır. İnternetin ilk olarak çıktığı günden bugüne kadar akan zamanla birlikte siber uzay, günlük yaşantımıza her geçen gün daha fazla entegre olmuştur. Evrensel bir ortam olan siber uzay, kendisine entegre olan ve sürekli genişleyen bir insan nüfusu tarafından etkilenen, interaktif, dinamik, gelişen, özgür, çok katmanlı bir fiziksel altyapıdan, yazılımlardan, regülasyonlardan, fikirlerden, yeniliklerden ve etkileşimlerden oluşan ekosistemdir. Siber uzay aynı zamanda insanlara sosyal hayatlarındaki kimliklerinin yanında başka bir kimlik edinebildikleri bir ortam olarak da dikkat çekmektedir.

Siber uzayın barındırdığı ve her geçen gün artan zafiyetlerden yararlanan ve bu potansiyeli kötüye kullanarak siber uzayı negatif etkileyen bir karanlık dünya bulunmaktadır. Siber uzayın oluşumundan beri varlığını sürdüren bu dünya, siber

uzayın kapsamının artmasıyla daha da büyümüş ve yaygınlaşmıştır. Bu karanlık dünyanın aktiviteleri esasen gerçek hayattaki gasp, hırsızlık ve aldatma gibi suçlardan farksızdır. Bu tür aktiviteleri gerçek hayattakilerden ayıran özellik, kullanılan farklı araçlar olarak çoğunlukla yazılımlar olması ve herhangi bir coğrafi engel bulunmamasıdır.

Karanlık tarafın büyümesine karşılık olarak pozitif gelişmeler de yaşanmıştır. Hem potansiyel hem var olan tehditler için yasalar ve düzenlemeler çıkartılmış hem engelleme hem de koruma amaçlı teknolojiler geliştirilmiş, güvenli kullanım ile ilgili dokümanlar, kılavuzlar çıkartılmıştır. Bunların en önemlisi de siber uzayın güvenliğini her açıdan ele alan siber güvenlik kavramı ortaya atılmıştır.

4.2. SİBER GÜVENLİK

Siber güvenlik kavramı, siber uzayın hayatımıza entegre olması ve bu uzay içerisindeki güvenlik endişelerinin ortaya çıkmasıyla oluşmuştur. Daha önce de sık sık gündeme gelen siber güvenlik 2009 yılında Amerikan Başkanı Barrack Obama'nın Amerikan halkını siber güvenliğin öneminin farkına varmaya ve ulusal güvenliğin sağlanması için bu konuda uygun etkinlikler ve eğitimler düzenleyeme davet etmesiyle popülerliği ciddi anlamda artmıştır. (The White House, 2009) Bilgisayar güvenliği, ağ güvenliği gibi daha alt dallarla sık sık karıştırılan fakat etki alanı çok daha geniş olan siber güvenlik kavramının her geçen gün popülerliğinin artmasıyla kapsamlı bir tanım yapılması zorunlu hale gelmiştir. Daniel Schatz, Rabih Bashroush, Julie Wall, "*Defining Cybersecurity*" adlı makalede, birçok makalede geçen siber güvenlik tanımlarının eksik yönlerini tespit ederek bu kavrama kapsamlı bir tanım getirmişlerdir: "Siber güvenlik, siber uzay içerisindeki varlıkların, organizasyonların, insanların ve verinin, gizliliğinin, bütünlüğünün, erişilebilirliğinin korunması için kurumlar ve devletler tarafından takip edilen güvenlik risk yönetimi süreçleriyle ilgili yaklaşım ve aksiyonlardır." (Schatz, Bashroush & Wall, 2017).

Tanımda belirtilen verinin gizliliği, erişilebilirliği ve bütünlüğü ilkeleri bilgi güvenliğinin temelidir ve literatürde CIA prensibi olarak tanımlanmaktadır. Siber saldırılar sonucunda genellikle bu üç prensipten biri veya birden fazlası istismar edilmektedir. Gizlilik ilkesi, hassas verilerin ve servislerin yanlış kişilerce erişilmesinin engellenmesinin gerektirir. Bilgiye ve servise erişim yetkisiz kişilere kısıtlandırılırken, yetkili kişilerce kullanıldığından emin olunmalıdır. Bütünlük ilkesi verinin tüm hayat döngüsü süresince doğruluğunun, tutarlılığının, güvenilirliğinin sağlanmasıdır. Veri, iletimi sırasında değiştirilmemelidir ve bununla birlikte yetkisiz kişilerce değiştirilmemesi için gerekli önlemler alınmalıdır. Erişilebilirlik, bir servisin erişilebilir olduğundan emin olunmasıdır. Bu ilke gereği bütün donanımların ve yazılımların sorunsuz bir şekilde çalıştığından emin olunmalıdır.

Siber güvenliğin kapsamı siber uzayın tamamıdır. Kasıtlı veya kaza eseri veya doğal bütün tehditlere karşı koruma sağlanması amaçlanır. Tanımda belirtilen süreçlerle ilgili aksiyonlar, yalnız tahmin edilebilir tehditlere karşı değil gerçekleşeceği tahmin edilemeyen tehditleri de içerir.

Siber uzaydaki fiziksel ve sanal sistemlerin güvenliğini kapsayan, aynı zamanda kriptografi, yapay zeka ve makine öğrenimi gibi bir çok bilim dalından yararlanan siber güvenliğe sadece teknik bir alan olarak yaklaşmak doğru olmayacaktır. Genel olarak bilgisayar biliminin bir alt dalı olarak görülen siber güvenlik, esasen birçok farklı alanı etkilemekte ve alt dallar içermektedir. Daha önce de belirtildiği gibi, siber güvenlik siber uzayı korumayı amaçlar. Siber uzayın değişmez parçalarından biri olan insanın, siber uzaydaki hareketlerinin, davranışlarının ve konumunun da siber güvenliğin bir konusu olduğu inkar edilemez. Siber güvenlik konusunda devletler yasalar çıkartır ve bazı politikalar uygular, devletlerle birlikte diğer organizasyonların da siber güvenlik stratejileri bulunmaktadır. Bu nedenle siber güvenliğin siyasal bilimlerle ve yönetim bilimleriyle de iç içe bir kavram olduğu açıktır.

Akıllı çözümleri ve bu çözümleri kullanacak insanlarıyla akıllı şehirler de siber uzayın bir parçası olacaktır. Geniş kaynakları ve yükselen potansiyelleriyle akıllı şehirlerin, siber uzayın karanlık tarafının da ilgi ve odak noktası olması beklenmektedir. Her türden cihazın ve insanların büyük çoğunluğunun internete bağlı olduğu bu şehirlerde gerçekleşecek bir siber saldırının etkisi büyük olacaktır. Başarılı olacak bir siber saldırı sonucunda kötü niyetli kişilerce şehrin kaynakları boşa kullanılacak, şehrin verimliliği düşecek, sistemler zarar görecek, gizli veriler kötü niyetli kişilerin eline geçecek ve şehrin işleyişi yavaşlayacak hatta durma noktasına gelecektir. Böylelikle daha yaşanılabilir, verimli ve sürdürülebilir bir yaşam sunmayı amaçlayan akıllı şehirler vadettiklerini sunamayacak ve akıllı şehir olmaktan uzaklaşacaklardır. Bu tür istenmeyen durumlarla karşılaşılmaması adına, akıllı şehirlerde de siber güvenliğin önemi kavranmalı ve sağlanması için gerekli aksiyonlar alınmalı ve en önemlisi şehrin her bir bireyinde siber güvenlik farkındalığı oluşturulmalıdır.

4.3. SİBER RİSK

Risk, istenmeyen bir olayın meydana gelme olasılığıdır. Daha önce tanımında da belirtildiği gibi siber güvenlik bir tür risk yönetim süreciyle ilgili aksiyonlar ve yaklaşımları içerir. Bu nedenle siber risk olarak tanımlanan bir risk türü ortaya çıkmıştır. Bu tür riskler siber uzayda işlenen, depolanan ve iletilen verinin gizliliğinin, erişilebilirliğinin ve bütünlüğünün kaybedilmesiyle, sistemlere yetkisiz erişim sağlanması, zarar verilmesi veya verilen hizmetlerin engellenmesi gibi durumlarda ortaya çıkar. Bir olasılık kavramı olan siber riski genel olarak sıfıra indirgemek pratikte mümkün olmasa bile amaç bu riski bütçe, zaman gibi kriterlere bağlı kalarak optimum seviyeye indirgemektir. Siber riski etkileyen iki faktör vardır. Bunlar siber atak olasılığı ve olası atağın etkisidir. Siber risk, bu iki parametreyle doğru orantılıdır. Siber risk, aşağıdaki formül ile formüllenebilir.

Siber Saldırı Olasılığı × Saldırının Olası Etkisi

Şekil 14 Siber Risk Formülü

Formülün detaylı olarak incelenebilmesi için öncellikle siber saldırı tanımlanmalıdır. Siber saldırılar, siber uzay içerisindeki bir veya birden fazla unsurdan, yine bir veya birden fazla unsura karşı gerçekleştirilen saldırılardır. Bu tür saldırılar, bireyler, toplumlar, organizasyonlar tarafından gerçekleştirilebileceği gibi devlet tarafından veya devlet destekli de gerçekleştirilebilir. Siber saldırıların en yaygın amaçları, saldırılan sistemin ele geçirilmesi, sistemin yok edilmesi, verinin sızdırılması veya saldırılan sistemin hizmet vermesinin engellenmesidir.

Siber saldırı olasılığı, zafiyetler, alınan önlemler ve tehditlere bağlı olarak değişmektedir.

Saldırının etkisi ise potansiyel kayıplarla ifade edilir. Bileşenlerinden de anlaşılabileceği gibi siber risk, kaçınılması gereken bir durumdur.

4.3.1. Tehditler

Tehditler, zarar verme potansiyeline sahip olaylar veya durumlar olarak tanımlanmaktadır. Siber uzayda birçok tehdit olmakla beraber, saldırganların sistemlerden gizli veri çalması, sistem yöneticisinin dikkatsizlik sonucu veri tabanını silmesi, politik nedenlerle sistemlere hizmet engelleme saldırıları düzenlenmesi, yangın çıkması sonucu sistemlerin tahrip olması gibi farklı örnekler gösterilebilir. (Muscat, 2017)

Siber tehditleri hayata geçirenler tehdit aktörleridir. Bu aktörler bu tehditleri gerçekleştirme potansiyeli olan kişi veya kuruluşlardır. Politik ve çevresel olaylar

genel olarak tehdit aktörü olarak kabul edilmese de bu nedenle oluşabilecek tehditlere de azami önem gösterilmesi gerekmektedir.

Tehdit aktörlerinin sınıflandırılmasında, aktörlerin çeşitli özelliklerinden faydalanılır. Bu özellikler motivasyon, bilgi toplama kabiliyetleri, teknik bilgi seviyesi ve kaynakların miktarıdır.

Saldırgan gruplar veya örgütlerin hareketlerinde, finansal, sosyal veya politik motivasyonları olabilir. Bireysel tehdit aktörlerinin, hacker toplulukları içerisinde ün kazanmak istemeleri, genellikle yöneticiler olmak üzere kişilere duyulan öfke gibi farklı motivasyonları da bulunabilir. Bu aktörlerin motivasyonları incelenerek çeşitli çıkarımlara varılabilir. Sabotaj, bilgi hırsızlığı, itibara zarar verme gibi stratejik amaçlar, hedef seçimi ve aktörün alacağı belirli teknik aksiyonlar motivasyonlar tarafından etkilemektedir.

Bir siber saldırının başarı ihtimali, saldırganın hedef hakkında topladığı bilgi miktarı ve değeri ile doğru orantılıdır. Saldırının hem öncesinde hem sonrasında bilgi toplamak mümkündür. Sistem hakkındaki en küçük bilgi bile atak vektörünü oluşturacak yapbozun kilit parçası konumuna gelebilir. Aşağıdaki bilgiler bir saldırı için büyük önem arz edebilir:

- Genel sistem mimarisi, servisler, kullanılan donanım ve yazılım bileşenleri ve konfigürasyon ayarları, ağ topolojisi ve kullanılan teknoloji
- Kullanılan güvenlik duvarı, anti-virüs, IDS gibi güvenlik mekanizmaları.
- Kullanılan bu teknolojik bileşenlerin bilinen zafiyetleri
- Sistemlerin veya servislerin kullanıcıları hakkında genel bilgiler ve erişim hakları

Saldırganın teknik bilgisi, toplanan bilgilerin başarılı bir saldırı senaryosuna dönüştürülüp uygulanarak tehdit oluşturulmasını sağlayacaktır. Saldırganın teknik bilgisi, toplayacağı bilginin niteliğini ve miktarını da arttıracaktır. Saldırgan teknik bilgi seviyesiyle bilinen zafiyetler hakkında tecrübe sahibi olabilir veya yeni

zafiyetler ortaya çıkartarak kullanabilir. Ayrıca topladığı bilgileri daha verimli çıkarımlar yapabilme kabiliyetine de sahip olabilir.

Aktörlerin ellerindeki kaynaklar da tehdidin boyutunu arttırabilir. Finansal kaynaklar çeşitli şekillerde verilecek zararın boyutunu arttırmada kullanılabilir. Bu kaynaklar rüşvet, fidye daha gelişmiş ve inandırıcı sosyal mühendislik çalışmalarında kullanılabileceği gibi, daha yetenekli kişileri saldırıya dahil etme, mevcut kişilerin kabiliyetleri arttırma, sıfırıncı gün istismarları, daha gelişmiş saldırı araçları veya daha fazla işlem gücü olarak değerlendirilebilir.

Tehdit aktörleri yukarıdaki parametrelere dayanarak:

- *Script kiddie:* Statü kazanma, kendini ifade etme gibi motivasyonları, sınırlı teknik yeteneği, sınırlı bilgi toplama kabiliyeti ve sınırlı finansal kaynağı bulunan, stratejik bir planlaması bulunmayan, kolay görünen hedefler seçen aktörlerdir.
- *Öfkeli çalışan:* Asıl motivasyonu intikam olan, bilgi toplama yeteneği eski veya mevcut çalışan olmasından ötürü bir miktar yüksek, teknik seviyesi yüksek olabilecek, finansal kaynakları limitli olan saldırganlardır. Bu aktörler kararlıdır ve hedeflerini düzgün bir şekilde belirlenmişlerdir.
- *Hacktivist gruplar: Belirli* bir politik veya sosyal ideolojinin savunulması veya yaygınlaştırılması gibi motivasyonları bulunan, bilgi toplama kabiliyetleri ve finansal kaynakları sınırlı, teknik bilgileri üyelere göre artıp azalabilen aktörlerdir. Adı medyada sıklıkla duyulan Anonymous grubu hacktivist gruplara bir örnektir.
- *Terörist organizasyonlar:* Motivasyonu ideoloji veya bir dini yaymak olan, bilgi toplama kabiliyetleri limitli, teknik seviyesi sınırlı fakat siber suç örgütleriyle bağlantılı olabilen, finansal kaynakları yüksek potansiyelli olan aktörlerdir.
- *Siber suç organizasyonları:* Günümüzde sıradan kullanıcılar, devletler ve kurumlar için en büyük siber tehdit aktörü olarak gösterilen siber suç organizasyonlarının genel motivasyonları maddi kaynaklıdır. Bu işi tam

anlamıyla profesyonel olarak gerçekleştiren bu organizasyonların saldırılarının her bir adımı planlıdır. Zaman aralığı ve atak yüzeyi oldukça geniştir. Teknik seviyeleri yüksek olan bu gruplar aynı zamanda en uzman hackerları işe alabilir, para karşılığında istismar kodları, zararlı yazılımlar ve saldırı araçları satın alabilirler. Finansal kaynakları potansiyel olarak geniştir.

- *Devlet destekli saldırganlar:* Temel motivasyonları devletin sosyal, politik ve ekonomik motivasyonlarıyla örtüşür. Hedefleri net, stratejik planları belli ve operasyonları uzun vadelidir. Bilgi toplama kabiliyetleri ve teknik seviyeleri en üst seviyededir. Devlet desteğini arkasına almış olan bu saldırganların finansal kaynakları sınırsız sayılabilir. Saldırı araçları, sıfırıncı gün saldırıları, zararlı yazılımlar satın alabilir, uzman hackerları işe alabilir veya yetiştirebilirler. Çin destekli APT1 ve NSA'in TAO grupları örnek olarak gösterilebilir.

Esas olarak bir tehdidin tamamen savuşturulması mümkün değildir. Bu noktada önemli olan zafiyetlerin doğru bir şekilde adreslenebilmesidir. Fakat bu tehditlere ve tehdit aktörlerine gereken önemin verilmesi zorunluluğunu ortadan kaldırmamaktadır. Tehditlerin ve zafiyetleri istismar edecek tehdit aktörleri hakkındaki analizler ve öngörüler zafiyetin ortadan kaldırılması veya riskin azaltılması için uygulanacak önlemleri büyük ölçüde etkileyecektir. Her zaman kolay bir süreç olmayan zafiyetin kapanması sürecinde, olası tehdit aktörleri tarafından istismar edilmesi mümkün olmayan zafiyetlere karşı koymak her zaman gerekli olmayabilir. Burada azami özen gösterilmesi gereken konu tehditlerin sıklıkla tekrar değerlendirilmesi gerekliliğidir.

4.3.2. Zafiyetler

Zafiyetler, sistemlerdeki zayıflıklar olarak tanımlanır. Bu zayıflıklar, olası atak vektörlerini oluşturarak saldırganlar için saldırı noktaları oluşturur. Tek bir zafiyetle büyük bir kayıp yaşanabileceği gibi birçok zafiyetin bir araya getirdiği bir atak vektörüyle sistemler istismar edilebilir. Zafiyetler, bir tehdit unsuru tarafından

istismar edilebileceği gibi, bir aktöre gerek kalmadan sistemlerde aksamalara sebep olabilir.

Zafiyetler dört temel başlık altında incelenir. Bunlar teknik, fiziksel, operasyonel ve bireysel kaynaklı zafiyetlerdir.

Teknik zafiyetler, donanımlar, yazılımlar, sistemler ve protokollerde bulunan dizayn kusurları ve uygulama hatalarıdır. Bu tür zafiyetler sonucunda sistemler üzerinde komut çalıştırılabilir, hizmet engelleme saldırısı gerçekleştirilebilir, veri sızıntısı yaşanabilir.

Fiziksel zafiyetler, sistemlerin uygun olmayan ortamlarda bulundurulmasıyla ortaya çıkar. Fiziksel saldırıya açık olan varlıklar çalınabileceği gibi ulaşılabilir olmaları nedeniyle kırma, koparma, kesme gibi yöntemlerle hizmet dışı bırakılabilir. Aynı zamanda nem, toz ve doğal afetlere karşı savunmasız kalan sistemler de hizmet veremez duruma gelebilir.

Operasyonel zafiyetler, sistemlerin sürdürülmesinde kullanılan prosedürlerdeki zafiyetlerdir. Bu tür zafiyetlerin oluşma sebepleri, sistemlerin düzenli olarak test edilmemesi ve denetlenmemesi, kritik verilerin belirlenmemesi, belirli standartların oluşturulup uyulmaması veya bulunmaması gibi sebeplerdir.

Bireysel zafiyetler: Bireyler, sistemlerin kullanıcıları ve şirket çalışanlarıdır. Yetersiz güvenlik farkındalığı ve işe alım, hizmet satın alma gibi süreçlerdeki eksikler nedeniyle yanlış kişilerin dahil olmasıyla ortaya çıkar.

Her geçen gün eski zafiyetler kapatılıyor olsa bile çıkan zafiyet sayısı da artan bir ivmeyle yükselmektedir. Zafiyetlere çözümler üretildikten sonra bile zafiyeti barındıran sistemler bulunmaktadır. Bu durumun belli başlı nedenleri bulunmaktadır:

- Her geçen gün daha da karmaşık hale gelen sistemlerde zafiyet bulunma riski artmaktadır.
- Kullanılabilirlik ve fonksiyonellik, güvenlik ile ters orantılı parametrelerdir. Maksimum güvenliğe sahip ürünlerin fonksiyonelliği ve kullanılabilirliği azalmakta bu nedenle satışı zorlaşmaktadır. Diğer parametreler için güvenlik tarafında verilecek tavizler, zafiyetlerin ortaya çıkmasına neden olmaktadır.
- Teknolojik ürünler için piyasaya çıkma tarihleri, bütçe gibi nedenlerden dolayı da gerekli kontroller en verimli şekilde yapılamamaktadır. Şirketler belirli aralıklarla yeni ürünler çıkartırlar. Yeni çıkan ürünlerle birlikte eski ürünlere verilen destek kesilir. Bunun sonucunda kullanımda olan zafiyetli ürünler saldırı noktaları oluşturur.
- Bilgi teknolojileri sistemleri insanlar tarafından dizayn edilmekte, uygulanmakta ve yönetilmektedir. İnsanlar karşılaştığı durumlar, yaşadığı olaylar ve doğası gereği hata yaparlar.
- Bilinen zafiyetli ürünlerin, yamalar çıkmış olmasına rağmen yama yönetimindeki ihmaller, saldırganlar için saldırı noktaları oluşturmaya devam etmektedirler.

4.3.3. Önlemler

Tehdit potansiyelini azaltmak, zafiyetleri kapatmak veya seviyesini düşürmek veya saldırıları engellemek, bertaraf etmek veya etkisini minimuma indirgemek için alınan aksiyonlar, prosedürler, cihazlar veya tekniklerdir. Temel amaç zafiyetleri kapatarak veya istismar edilme potansiyelini düşünerek, analiz edilen tehdit aktörlerinin tehdit oluşturmasını engellemek olduğundan, zafiyetler başlığındaki dört temel maddede incelenebilir.

Alınacak teknik önlemler ağ ve ağa dahil cihazlar için güvenlik kontrolleridir. Dijital erişimin sınırlandırılması amaçlanır. Bunlara örnek olarak güvenlik duvarları, anti-virüs yazılımları, şifre üreticiler, güvenlik protokolleri, güvenli ve güçlü kriptografik algoritmalar gösterilebilir.

Fiziksel önlemler alınarak cihazlara fiziksel erişimin sınırlandırılması, cihazların doğal afetlerden ve çevresel faktörlerden korunması hedeflenir. Sunucu odalarının yeterli derecede soğutulması, kilitler, çitler, kurcalamaya karşı korumalı donanımlar örnek olarak verilebilir.

Operasyonel önlemler insanların yönetimi ve sistemlerin çalışması ile ilgili oluşturulacak ve uygulanacak politikalar ve prosedürleri kapsamaktadır. Teknik taraf için parola değiştirme politikası, anahtar yönetimi prosedürleri, belirli aralıklarla güvenlik testleri yapılması, personel tarafı için işe alım ve işten çıkartma gibi prosedürlerin düzenlenmesi örnek olarak gösterilebilir.

Bireysel önlemler, güvenlik farkındalığının ve insanların güvenilirliğinin arttırılmasına odaklanan önlemlerdir. Çeşitli eğitimler düzenlenmesi, çalışan memnuniyetinin arttırılması ve iş yerinde adaletin sağlanması örnek verilebilir.

BEŞİNCİ BÖLÜM

SİBER ZAYIFLIKLAR BAĞLAMINDA DİKKAT EDİLMESİ GEREKEN KONULAR

5.1. KİŞİSEL VERİLERİN KORUNMASI

Kişisel veri kavramı, kanunda "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" şeklinde tanımlanmıştır (KVKK, 2016). Bireyin adı, soyadı, anne adı, baba adı, doğum tarihi, doğum yeri gibi teşhis edici bilgilerin yanı sıra ev adresi, fotoğrafı, e-posta adresi, banka bilgileri, sosyal medyadaki paylaşımları, tıbbi bilgileri veya bilgisayarının IP adresi gibi fiziksel, fizyolojik, ekonomik, kültürel, sosyal veya psikolojik pek çok bilgiyi de içerir.

Güncel web teknolojileri ve akıllı telefonların ortaya çıkmasıyla, kişisel verilerin işlenmesinin, mevcut yönetmeliklerde dikkate alındığından çok daha karmaşık olduğu ortaya çıkmaya başladı. Temel olarak, konum paylaşım uygulamaları ve web üzerindeki kişisel sosyal paylaşımlar serbestçe kullanılabilen kişisel veriler karşılığında kolaylık ve fiyat avantajları ilkesine dayanan dijital bir endüstrinin büyümesine yol açmıştır.

Bulut bilişimin piyasaya sürülmesiyle birlikte, giderek artan bir şekilde ortaya çıkan bir soru, çok uluslu ve bağlantılı BT işlemlerinde, yasal düzenlemelere uyumu kontrol etme kapasitesinin, farklı yasal ortaklarla birlikte nasıl tasarlanabileceğiyle ilgilidir. Karmaşık mevcut Avrupa veri koruma yasalarını anlamak zaten yeterince zordur. Bununla birlikte, AB üyesi ülkeler arasında genellikle küçük ama yine de önemli farklılıklar ile birlikte ele alındığında, baştan itibaren uygun yasal destek sağlanmıyorsa, neredeyse kabul edilemez zorluklar ortaya çıkabilir.

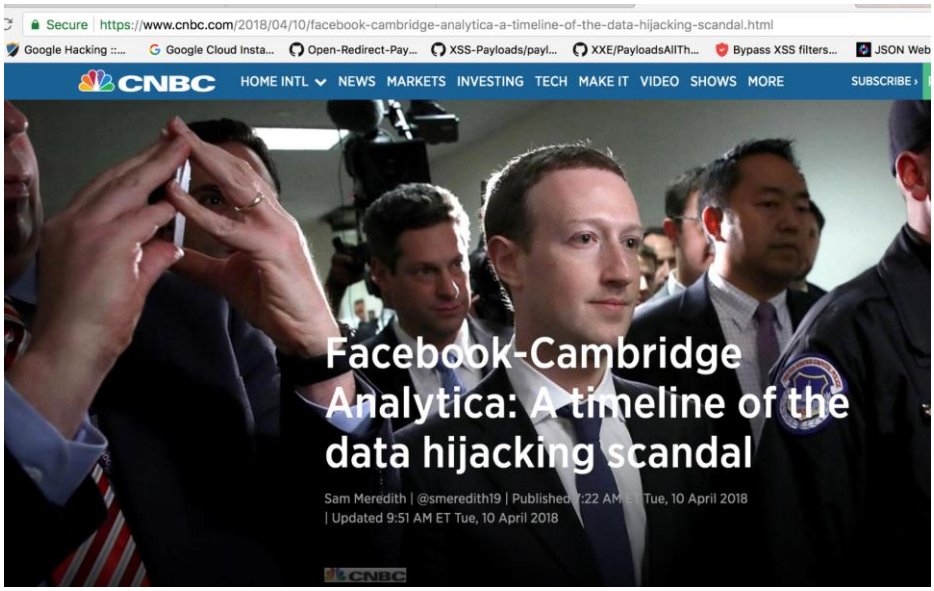
Verilerin artık dijitalleşmesi, güncel web teknolojileri, bulut bilişim birçok teknolojilerinin sağladığı yararlar yanında saklanan veya iletilen kişisel verilerin yanlış kullanımıyla ilgili riskler de vardır. Kişisel verilerin kullanımı ile mahremiyetin korunması arasındaki doğru dengeyi bulmak, dijital çağın en büyük

zorluklarından biridir. Mayıs 2018 itibariyle Avrupa Birliği içinde kişisel verileri işleyen tüm kuruluşlar, Genel Veri Koruma Yönetmeliği'nde (GDPR) belirtilenler de olmak üzere yeni kurallarla uğraşmak zorunda kalacaklardır.

Türkiye'de ise 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), 24.03.2016 tarihli Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Bu kanununa göre; ad, soyadı, ev adresi, telefon numarası, e-mail adresi, vatandaşlık numarası gibi kişisel veriler ilgili kişilerin izni olmadığı sürece işlenmeyecektir. Kurumların kişisel verileri nasıl kullandıklarını daha fazla kontrol etmeyi amaçlamakta ve kurallara uymayan organizasyonlara veri ihlali sonucunda ciddi cezalar getirmektedir.

Şehirlerin, hizmetleri daha hızlı, ucuz ve memnun edici şekilde sunmak için teknolojiye bağımlı hale gelmesiyle, verilere olan ihtiyaçları da artacaktır. Bunun mantıksal sonucu, veri korumanın her zamankinden daha önemli hale gelmesidir. Akıllı şehirde, kullanıcı verileri, her şeyi akıllı yapmak için elektronik cihazlarda saklanır. Bir akıllı telefon en çok kullanılan elektronik cihazdır ve tüm akıllı sistemlerin pivotudur. Bununla birlikte, mevcut akıllı telefonlar kullanıcıların hassas verilerini yönetmek için yeterli değildir ve veri fazlalığı nedeniyle ortaya çıkan gizlilik problemi ile karşı karşıyadır. Fazladan veri toplama, akıllı telefon uygulamalarının, kullanıcılara izin verildikleri süre içinde orijinal işlevinden daha fazla veri topladıkları anlamına gelir.

Endüstri 4.0, yapay zeka ve nesnelerin interneti konuları bütün dünyanın gündemini oluşturmaktadır. Yaklaşan IoT (nesnelerin interneti) devrimi ile 2018 yılına tahmini 11 milyar cihazla başlayacağımızı söyleyen Gartner, bu sayının önümüzdeki iki yıl içinde neredeyse iki katına çıkacağını ve 2020 yılına kadar dünyada 20 milyar "şeye" ulaşacağını tahmin eder ve bu sistemlerin akıllı şehirdeki en ciddi potansiyel güvenlik tehlikelerinden biri haline geleceğini göstermektedir (Gartner, 2017).



Şekil 15 Facebook-Cambridge Analytica Veri Sızıntı Skandalı Haberi

(CNBC, 2018)

5.2. DİJİTALLEŞMİŞ NESNELERİN HACKLENMESİ

Hackleme kelime anlamı olarak, dijital bir nesne, sistem veya ağda bulunan zafiyetler sonucunda yetkisiz bir şekilde giriş yapmak olarak tanımlanır. Kullanılan zafiyetler, sistem veya nesnelerdeki zafiyetler olabileceği gibi insan kaynaklı zafiyetler de olabilir. Hacklenmek ise hackleme işleminden etkilenme durumudur. Hacklenme sonucunda hacklenen nesne, sistem veya ağa yetkisiz kişilerce erişim sağlanır ve birçok amaç için kullanılabilir.

Hackleme işlemini gerçekleştiren kişiler ise hacker olarak tanımlanır. Hackerlar, hedeflerine erişebilmek için teknik bilgilerinin yanında sosyal becerilerini de kullanırlar. Kaba kuvvet, sosyal mühendislik, parola kırma, sahtekarlık (spoofing), halka açık exploitler, zararlı yazılımlar, aradaki adam (MitM), hizmet engelleme gibi birçok yöntem hackerlar tarafından yaygın bir şekilde kullanılmaktadır. Hackerlar yaptıkları işlemlerdeki amaçlarına göre üç temel gruba ayrılırlar.

Birinci grup hackerlar veya şapkalı (white hat) hackerlardır. İyi niyetli ya da etik hackerlar olarak da tanımlanan bu grup, hackleme işlemini iyi bir niyetle

gerçekleştirmektedirler. Bilgi ve yeteneklerini iyi amaçlar için kullanmaktadırlar. Beyaz şapkalı hackerlar, yazılı olarak izin aldıkları sistemler üzerinde sızma testi (Penetration Test) gerçekleştirirler. Bu testlerde beyaz şapkalı hackerlar, kötü niyetli bir kullanıcının kullandığı yöntemlerle dijital nesneleri hacklemeye çalışırlar. Bu testlerin amacı, test yapılan sistemler üzerindeki zafiyetlerin keşfedilip raporlanarak, kötü niyetli kişilerden önce önlem alınmasını sağlamaktır. Aynı zamanda zayıflık değerlendirmesi (vulnerability assessment) gerçekleştirerek, bulunan zafiyetlerin tanımlanmasını, ölçeklendirilmesini ve derecelendirilmesini yapmaktadırlar. Yapılan işlemlerin her biri yasal çerçeve içerisinde gerçekleştirilmektedir.

Siyah şapkalı hackerlar (black hat), kötü niyetle kasti olarak sistemler veya ağ üzerinde yetkisiz erişim sağlamak amacıyla hackleme işlemini gerçekleştirirler. Verileri çalma, kötü amaçlı yazılımların dağıtılması, fidye yazılımla fidyecilik, zararlı içerik veya siyasal bir görüşün yayılması, hizmet engelleme, şöhret elde etme gibi amaçları olabilir. Yapılan işlemler yasadışı kabul edilir ve suç olarak değerlendirilir.

Bir diğer grup ise gri şapkalı (gray hat) hackerlardır. Siyah şapkalı ve beyaz şapkalı hackerların arasında bir konumu bulunan bu tip hackerlar sistemlerde bulup istismar ettikleri açıkları siyah şapkalı hackerlar gibi kötü amaçlarla kullanmak yerine ilgililere raporlamaktadırlar. Yapılan işlemler beyaz şapkalı hackerlarda olduğu gibi yazılı izinle gerçekleştirilmemektedir.

Dijital nesnelerin kötü bir amaçla hacklenmesi, masum insanlar, şirketler ve devletlere karşı birçok kötü sonuç doğurabilir. Görünen sonuçların yanında uzun vadeli zararlar da göz önüne alınmalıdır.

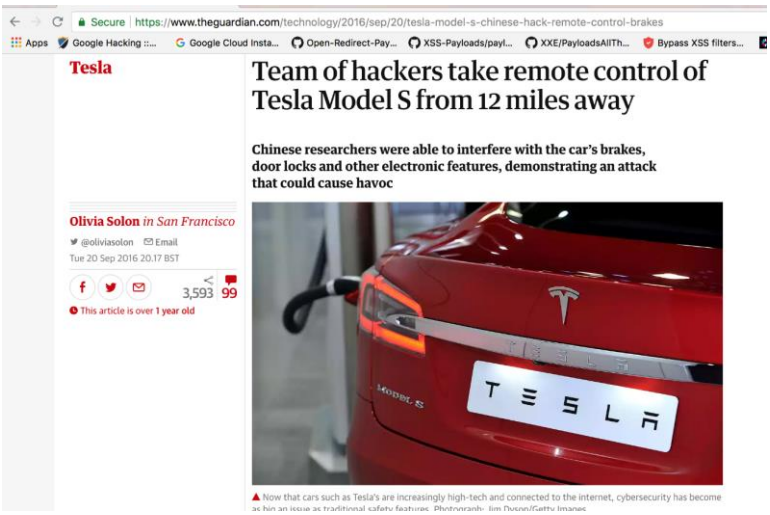
Hacklenme sonrasında hedef nesnelerin kontrolü tamamen veya kısmen hackerın kontrolüne geçebilir. Hacker bu cihazları kendi yararına veya başka kişi veya

kurumlara zarar vermek için kullanabilir. İşlemlerini, saldırının kurbanı kişilerin adına gerçekleştirerek kimlik sahtekarlığı yapabilir.

Bir diğer etkisi kişisel veya kurumlara özel verilerin ele geçirilmesidir. Bu çalınan bilgiler açığa çıkartılabileceği gibi kimlik sahtekarlığı için kullanılabilir ya da başka kişilere satılabilir. Ele geçirilen sistemler üzerindeki dosyalar şifrelenerek fidyecilik yapılabilir. Kişi veya kurumlara özel hesapların banka hesapları, veri tabanları ele geçirilerek büyük ekonomik etkiler yaratılabilmektedir.

Hackleme işleminin amacı kişi veya kurumlar üzerinden kar sağlamak olabileceği gibi kurumları dolaylı veya doğrudan zarara uğratmak da olabilir. Sistemlere kalıcı veya geçici hasar vererek hizmet vermelerini engelleme ve sistemler üzerindeki veriler silinerek maddi zarar verilebileceği gibi tamamen kişisel hırslarla sistemler ele geçirilerek kurbanlar zarara uğratılabilir.

Kurum ve bireyler hacklenme sonrasında itibar kaybına uğrayacaklardır. Özellikle güvenilirliğini kaybedecek olan organizasyonlar doğrudan aldıkları maddi zararın yanında dolaylı olarak da büyük zarara uğramış olacaktır. Hem kişiler hem de kurumlar her zaman hacklenmeye karşı hazırlıklı çoğu zaman kaçınılmaz olan hacklenme durumlarını en az zararla atlatabilecek seviyeye gelmelidir.



Şekil 16 Tesla Araçların Hacklenmesi Haberi

(The Guardian, 2016)

5.3. SİBER SUÇLAR

Teknolojik gelişmeler, insan hayatına pozitif yenilikler getirdiği gibi birtakım sorunları da beraberinde getirmiştir. Her geçen yıl daha da büyüyen siber uzay, gerçek hayatta karşılaştığımız birçok suç türüyle birlikte yeni türlere de sanal olarak ev sahipliği yapmaktadır. Bu uzayda gerçekleşen suçlara siber suçlar denmektedir. Siber suçlar elektronik iletişim kanalları ve bilişim sistemleri kullanılarak gerçekleştirilen yasadışı eylemlerdir. Bu eylemler, suçlular tarafından genel olarak kar amaçlı olarak icra edilse bile, bir kısım suçlular hedef olarak diğer sistemlere zarar vermeyi ve hizmet dışı bırakmayı belirlemektedir. Bir diğer grup ise zararlı yazılım, yasadışı bilgiler, resim veya materyalleri yaymak için ya da bu sayılan aktivitelerin birkaçını veya hepsini birlikte gerçekleştirmektedir. (Gordon & Ford, 2006). Siber suçlarda bilişim teknolojileri amaç olabildiği gibi araç da olabilmektedirler.

Siber suçları bu kadar yaygınlaştıran belli başlı sebepler vardır. Bunların başlıcası belki de en önemlisi internet üzerinde çok değerli kaynakların bulunmasıdır. Sınırsız miktarda veri, işlemci gücü, bankacılık, alışveriş gibi internet üzerinden verilen servisler bunlara örnek olarak verilebilir. İnternet üzerinde gerçek para ile yapılan işlemler özellikle kar amacıyla çalışan siber suçluların ilgi noktası haline gelmektedir.

Suçun Nevi Ve Yıllara Göre Olay Sayıları	*Kredi Kartı Sahteciliği ve Dolandırıcılığı*	*Banka Dolandırıcılığı*	*Bilişim Suçları ve Dolandırıcılığı*	*İnternet Aracılığıyla Dolandırıcılık*	*Diğer*	*Toplam*
Olay Sayısı 2003	*80*	*15*	*X*	*X*	*X*	*95*
Olay Sayısı 2004	*146*	*22*	*16*	*X*	*X*	*184*
Olay Sayısı 2005	*195*	*9*	*91*	*X*	*X*	*295*
Olay Sayısı 2006	*122*	*98*	*4*	*X*	*X*	*224*
Olay Sayısı 2007	*594*	*642*	*416*	*X*	*91*	*1.743*
Olay Sayısı 2008	*830*	*1.177*	*560*	*X*	*157*	*2.742*
Olay Sayısı 2009	*1.511*	*550*	*353*	*412*	*45*	*2.871*
Olay Sayısı 2010	*1.131*	*151*	*972*	*71*	*28*	*2.353*
Olay Sayısı 2011	*1.772*	*141*	*1.738*	*111*	*31*	*3.793*
Olay Sayısı 2012	*1.724*	*264*	*3.669*	*278*	*783*	*6.718*

Tablo 1 Türkiye'deki 2003-2012 Yılları Arası Siber Suç Sayıları

(Taşçı & Can, 2015)

Bir diğer önemli nokta ise internet üzerinden erişilebilir birçok cihaz ve sistem bulunmasıdır. Bu kadar geniş bir ağ üzerinde bulunan milyonlarca cihaz saldırı yüzeyini devasa boyutlara taşımaktadır. Bu boyuttaki bir yüzeyde her türlü teknik seviyeden ve her yaş grubundan bireyler bulunmaktadır. Güvenlik farkındalığı düşük kişilerce yönetilen sistemler, kullanılan bireysel cihazlar, taşıdıkları bilinen zafiyetler ve hatalı yapılandırmalarla açık hedef haline gelmektedirler. İnternete bağlı olması yeterli olan bu suçlular coğrafi konularından bağımsız olarak eylemlerini gerçekleştirebilmektedirler. Ayrıca onion routing, bullet-proof hosting gibi yöntemlerle kimliklerin kolayca gizlenebilmesi ve kullanılan araçlar ve çalınan verilerin gizli tutulabilmesi siber suçların daha da çekici bir hale gelerek yaygınlaşmasındaki bir başka sebeptir.

Siber suçlardaki artışın bir diğer nedeni ise hedeflerin bulunduğu ve saldırganın bulunduğu konumların farklı olmasıdır. Mahkemelerin ve yerel kolluk güçlerinin yargılama yetkisi sadece bulunduğu bölge için geçerli olması sebebiyle siber suçluların ceza almadan kurtulmaları, fiziksel olarak gerçekleştirilen suçlara göre çok daha düşüktür. Bununla birlikte yasalar ülkeden ülkeye değişmektedir. Özellikle Afrika ülkeleri yasaları siber suçlar karşı yetersiz kalmakta ve suçlular tarafından tercih edilen ülkeler haline gelmektedir. (Jackson, 2015)
Siber suçlarda sadece bir suç formundan yararlana bilineceği gibi birden fazla formun bir araya gelmesiyle bileşik formlarda oluşturulabilmektedir. Hollanda hükümetine göre en yaygın siber suç formları:

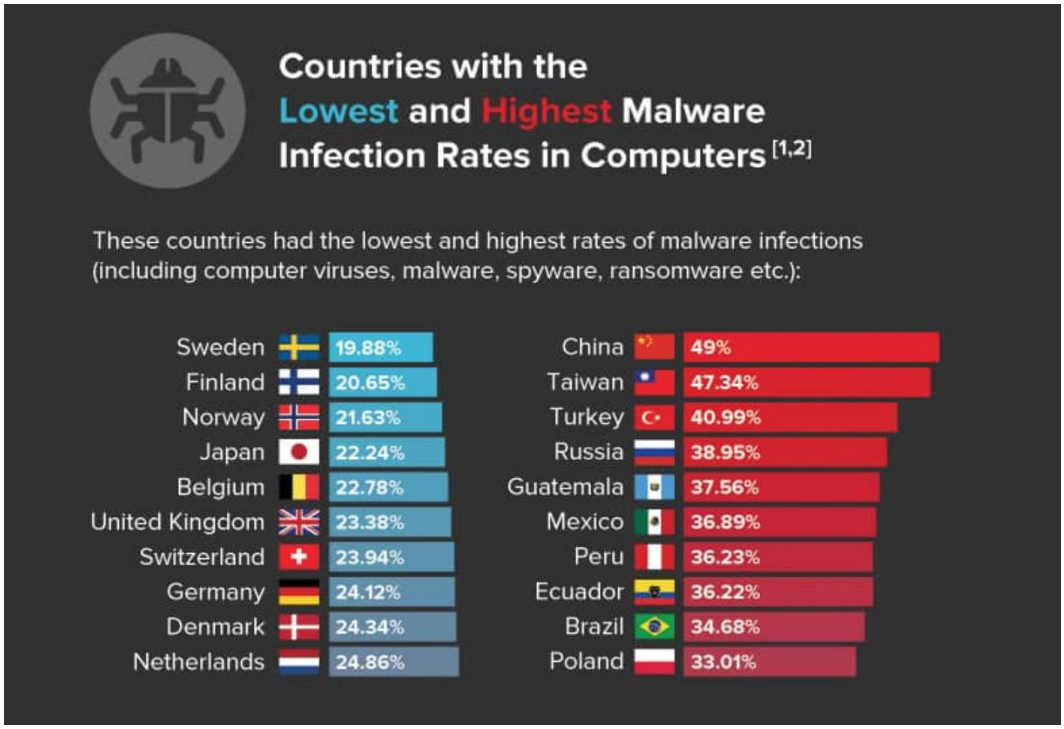
- Oltalama
- Kimlik hırsızlığı
- Hackleme
- Teröre teşvik etme
- Çocuk pornosu dağıtımı
- Çocukları kandırmaya yönelik eylemler

Şeklinde sıralanmıştır. (Government of the Netherlands, 2016) Siber suç dünyası ekonomisi, “cybercrime underground” adı verilen siber suçluların yeraltı ortamda

yürümektedir. Deep Web (Derin ağ) üzerinde yani standart web tarayıcılarıyla erişilemeyen bir katmanda hizmet veren bu dünyada çeşitli aktörler bulunmaktadır. Bu aktörler siber yeraltında bir araya gelerek karşılıklı çıkar ilişkisiyle ticaret gerçekleştirmektedirler. IRC ağları, sosyal medya, forumlar, Tor gibi anonim iletişim sistemleri üzerinden haberleşme sağlanan bu markette para birimi genellikle Bitcoin kripto paralardır. Bu dünyadaki aktörler ve sattıkları ürünler aşağıda listelenmiştir:

- *Bilgi tüccarları:* Müşteri ve hesap bilgileri, kredi kartı numaraları gibi bilgilerin yanında sistemler üzerindeki bilinen zafiyet bilgileri gibi değerli bilgiler satmaktadırlar.
- *Kaynak tüccarları:* İşlemci veya insan gücü satmaktadırlar. Botnet oluşturma ve genişletme, hacker brokerliği gibi hizmetler satmaktadırlar.
- *Servis sağlayıcılar:* Bullet-proof hosting adı verilen bir sunucu hizmeti vermektedirler. Bu sunucular siber suçlular için güvenli liman kabul edilen ülkelerde bulunmakta ve suçlular tarafından zararlı içeriklerin depolanması için kullanılırlar. Bunun yanında VPN, proxy gibi servisler, bunlara ek olarak hizmet engelleme ve hackleme hizmetleri de satmaktadırlar.
- *Ar-ge işçileri ve araç yapımcıları:* Zararlı yazılımlar, istismar kodları, hizmet engelleme araçları gibi saldırı araçları geliştirerek satmaktadırlar.
- *Suçlular, dolandırıcılar ve saldırı başlatıcılar:* Hizmet ve ürün satın alan ve saldırıları başlatan aktörlerdir.
- *Kasiyer veya para kuryesi:* Kara para aklayan aktörlerdir. Parayı ülkeler ve banka hesapları arasında gezdirerek takip edilmesini zorlaştırmaktadırlar.

Günümüzde siber suçlular sistemli bir şekilde hareket etmekte ve takip edilmeleri giderek zorlaşmaktadır.



Şekil 17 Dünya'da En Az ve En Fazla Zararlı Yazılıma Maruz Kalan Ülkeler Sayısı

(O'Driscoll, 2018)

ALTINCI BÖLÜM

SİBER SALDIRI SENARYOLARI

Siber saldırılar sonucunda akıllı şehirlerde büyük veya küçük çaplı olumsuz etkiler olacaktır. Siber saldırıların olası sonuçları olan sistemlerin kısmen veya tamamen ele geçirilmesi, veri sızıntısı, şehir işleyişinin durması ve hatta insanların canına ve sağlığına gelecek doğrudan sonuçları olduğu gibi farklı saldırıları için uygun koşul yaratılması gibi doğrudan gözlenemeyecek sonuçları da olabilir. Güvenlik önlemleri yeterli olmayan şehirlerde saldırıların sonuçları daha ağır olacaktır. Çok küçük bir cihazın ele geçirilmesiyle ağa dahil saldırganlar bütün şehir sistemleri üzerinde kontrol sahibi olabilirler.

6.1. MOBİL CİHAZLAR VE DİJİTAL PLATFORMLAR

Mobil cihazlar ve bu cihazlar üzerinden erişilen dijital platformlar ve uygulamalar bulundurdukları zafiyetlerle birçok saldırı tipine maruz kalabilir. Saldırganlar uygulamanın akışını hedef alabileceği gibi uygulama sunucularındaki verileri de hedefleyebilir. Akıllı şehirlerde insanlar, yapacakları işler ve birtakım tercihler konusunda mobil cihazlarına kuracakları uygulamalar üzerinden edinecekleri bilgilere danışabilirler. Aynı zamanda bu dijital platformlar, kullanıcıları yöneticilerle buluşturan platformlar olma özelliği de taşıyabilir. Bu nedenle bu alanda yapılacak saldırılar, verilerin çalınmasına, insanların ve yöneticilerin yanıltılmasına sebep olabilir.

Örnek olarak hacklenen bir toplu taşıma uygulamasında, saldırganlar birçok aracın servis dışı olduğu bilgisini paylaşabilir. Bu yanlış bilgi sonucunda şehirdeki binlerce insan kişisel araçlarıyla trafiğe çıkacak trafik yoğunluğu artacak ve işler aksayacaktır.

İnsanların görüşlerinin birer formla alındığı platforma yapılacak bir sınırsız form gönderimi saldırısıyla saldırganlar, anket sonuçlarını manipüle ederek kendi istedikleri kararın alınmasına sebep verebilir.

6.2. BÜYÜK VERİ VE AÇIK VERİ

Şehirlerde herkese açık çok büyük miktarda veri bulunmaktadır. Bu veriler iyi niyetli insanlara açık olduğu gibi saldırganlara da açıktır. Veri koruma ve inovasyon arasındaki denge iyi ayarlanamazsa, açık veri insanların alışkanlıkları, bulundukları veya bulunacakları mekanlar, zamanlamalar ile ilgili bilgiler sızdırabilir. Bu durumun bir sonucu olarak, bir siber saldırı hatta bir terör saldırısı için en uygun zaman, en uygun mekân gibi bilgiler, açık veriler üzerinden elde edilebilir.

6.3. NESNELERİN İNTERNETİ

Herhangi bir saldırı durumunda şehri belki de en derinden etkileyecek olaylar bu konsepte gerçekleşecek bir saldırı senaryosudur. Şehirdeki elektronik cihazların büyük bir çoğunluğu internete bağlı olarak çalıştığı için, bu saldırıların büyüklü küçüklü birçok etki yaratması olasıdır. Örnek olarak IoT altyapısıyla yönetilen bir trafik yönetim sisteminin bir siber saldırıyla ele geçirilmesi büyük felaketlere yol açabilir. Trafik ışıklarını kontrol eden saldırganlar, trafik kazalarına sebep olarak birçok insanın ölümüne neden olabilir.

Akıllı şebeke çözümleriyle verimli enerji kullanan akıllı şehirlerde, bu sistemlerin hacklenmesiyle şehrin kaynakları gereksiz bir şekilde harcanabilir. Bu durum hem şehir ekonomisine hem de doğaya zarar verecektir.

Akıllı şehirlerde birçok çözüm, internet üzerinden haberleşen sensörler aracılığıyla sağlanmaktadır. Bu sensörlere yapılacak saldırılarla, gerçek dışı veri üretimi gerçekleşen senaryolar yaşanabilir. Saldırganlar sahte deprem, silahlı saldırı, sel gibi felaket alarmları alarak şehirde panik havası yaratarak dikkat dağıtıp, farklı saldırılar gerçekleştirebilir.

Şehirdeki belediye ekipleri de internete bağlı cihazların gönderdiği uyarılarla çalışmaya başlayacaktır. Örnek olarak, boşaltılması gereken çöp konteynırları sinyal gönderecek, hırsızlık tespit eden hava araçları kolluk kuvvetlerine alarm üretecektir. Bu alarmları üretecek cihazların hacklenmesi ve yanlış alarm üretilmesiyle, belediye çalışanları, polis gibi personelin yanlış alarm durumuna düşmesine sebep olacaktır. Özellikle farklı noktalara gönderilerek polis ekiplerinin dikkatinin dağıtılması, şehir için daha farklı güvenlik riski yaratacaktır.

6.4. 3 BOYUTLU BASKI

Üç boyutlu baskı cihazları, üretim sektörünü baştan aşağı değiştirecek ve insan hayatına önemli katkılarda bulunacaktır. Çalışabilmesi için birçok farklı kaynak kullanan ve her türlü nesnenin üretilmesini mümkün hale getiren bu cihazların, saldırganların radarına girmesi de kaçınılmaz olmuştur. Hackerlar sadece dijital olarak birçok şey elde edebileceği gibi bu cihazlarla birlikte akıllı şehirlere karşı tehditler daha çok fiziksel boyuta taşınmıştır.

Üç boyutlu baskı cihazlarının ele geçirilmesiyle, cihazın kullanım amacına göre saldırganlar diledikleri objeleri üreterek kullanabilir hale geleceklerdir. Üretecekleri cihazları, farklı saldırı senaryolarında da kullanabilirler. Bu saldırıların bir diğer ayırt edici özelliği de örneğin mobil cihazlardan farklı olarak mekanik bir sistem olarak çalıştığından, sonuçların tespiti bir miktar daha zordur. Örneğin çalınan bir kredi kartı bilgisinin sonucu kolay bir şekilde tespit edilebiliyorken hatalı üretilecek bir ürünün verebileceği zarar satışından sonrası bir zaman diliminde gözlemlenecektir.

Yeni ürünler üretilebileceği gibi mevcut ürünlerin de manipüle edilmesi mümkündür. Örnek olarak manipüle edilecek, koruyucu kask, bebek koltukları benzeri güvenlik amaçlı ürünlerin olması gerektiği gibi üretilmemesi can kaybı veya yaralanmalarla sonuçlanabilir.

Bunlara ek olarak bu cihazların sunucuları ele geçirilerek, sahte materyal siparişi verilerek kaynakların verimsiz kullanımına sebep olunabilir. Sadece ekonomik zarar vermek yerine ekonomik fayda da elde etmek isteyen saldırgan bu ürünleri kendi adresine gönderebilir.

6.5. SOSYAL ETKİLEŞİMLİ ROBOTLAR

Akıllı şehirlerde hizmet verecek robotların, gerekli hizmetleri verebilmeleri için kritik veriler depolayan veri tabanı sunucularıyla sürekli olarak iletişim halinde olacaklardır.

Bu robotların ele geçirilmesiyle, kritik veri tabanlarına da erişim sağlanmış olacak ve elde edilecek bilgilerle sosyal ve ekonomik birçok zarar ortaya çıkacaktır. Ya da müşteriler yanlış yönlendirilerek saldırganların emellerine hizmet edeceklerdir. Örneğin belediye binasında çalışan bir robot müşteriden kişisel verilerini alıp saldırganlara ileterek, kimlik hırsızlıklarına neden olabilir. Ya da saldırganlar bu robotlarla sosyal mühendislik çalışması yapmadan da direkt olarak veri tabanı sunucularından bu bilgileri alarak kolaylıkla farklı saldırılarda kullanabileceklerdir.

Veri toplama ve işleme gibi dijital, araç ve gereç kullanma gibi mekanik birçok özelliği bulunacak olan bu robotlar, hacklenerek saldırganlar için fiziksel bir silaha dönüştürülebilir, canlı ve cansız şehir unsurlarına zarar verebilir.

Hacklenen robotların verebileceği zararlar sadece fiziksel değildir. Eğitimde de git gide yaygınlaşan robotların, öğrencilere vereceği yanlış bilgiler ve sosyal zararlar gelecek için çok daha büyük felaketlere yol açacaktır.

6.6. İNSANSIZ ARAÇLAR

Küçük ve büyük birçok insansız araç, akıllı şehirlerde yolcu taşımacılığı, kargo, izleme, alarm üretme ve müdahale gibi farklı alanlarda kullanılmaktadır.
Bu araçlara yapılacak saldırılar da felaketle sonuçlanabilir.

Kargo için kullanılan bir aracın ele geçirilmesiyle saldırgan kargoyu kendi adresine yönlendirebilir. İzleme yapan bir araçla bilgi toplayabilir, yolcu taşımacılığı yapan araçlar ile trafikte kaosa neden olup şehre zarar verebileceği gibi insanlara da zarar verebilir. Ayrıca ele geçirilen bu cihazlar silahlandırılarak birer savaş makinesine dönüştürülebilir.

YEDİNCİ BÖLÜM

AKILLI ŞEHİRLERDE SİBER GÜVENLİK VE TAKİP EDİLMESİ GEREKEN PRENSİPLER

7.1. AKILLI ŞEHİRLERDE KARŞILAŞILABİLECEK SİBER GÜVENLİK PROBLEMLERİ

7.1.1. Akıllı Şehirlerdeki Genel Siber Güvenlik Problemleri

Siber güvenlik bağlamında akıllı bir şehirde temel gereklilikleri belirlemek sorun olabilecek alanları daha iyi teşhis edebilmek açısından önemlidir. Akıllı şehirdeki siber güvenlik çoğunlukla yönetişim faktörleri, sosyo-ekonomik faktörler ve teknolojik faktörler olmak üzere üç faktöre bağlıdır. Bu faktörler, akıllı bir şehirde siber güvenlik için bir araya getirilerek teknoloji ile yönetilebilir. Akıllı şehirlerde karşılaşılabilecek temel güvenlik problemleri anlatmadan önce birkaç temel kavramın üstünde durulması gerekir.

İlk olarak, kişisel veriler akıllı bir ortamın atomu gibidir. Akıllı şehirleri oluşturan temel parçacıklardır. Veriler, şehri akıllı yapmaz, ancak şehrin zekâsını oluşturur. Başka bir deyişle, kentsel hizmetlerin akıllı olması, ulaşım, enerji ve su gibi hizmetlerini optimize edebilmeyi sağlar.

İkinci olarak, akıllı şehirlerin dinamiği dramatik bir biçimde değişmiştir. İlk akıllı şehirler genellikle politik ve idari gücün olduğu şehirlerdi. Dinamikler; kendilerini, vatandaşlar ve kent yönetimindeki paydaşlar arasında konumlandıran özel ya da ortak paydaşların gelişiyle değişti. Yeni bir dinamik yaratan bu yeni ara yüz ile daha az planlı fakat daha yenilikçi bir manzara ile karşı karşıyayız.

Üçüncü bakış açısı daha özel olarak kamu gücünün ve kamu hizmetlerinin rolüne atıfta bulunmaktadır. Açık veri politikalarının ve genel faiz verilerinin artması, kentsel kamu hizmetleri üzerinde potansiyel olarak çok olumlu bir etkiye sahip olmuştur: süreklilik, kalite ve evrensellik. Kamu ve özel sektör arasındaki bu

bağlantı, aslında hizmet kalitesinin, evrenselliğin ve sürekliliğin sağlanmasına katkıda bulunabilir.

Taşımacılık sektörü en iyi örneklerden bir tanesidir. Veri kullanımı; hat değişimini önleyerek ve yolculara çeşitli ulaşım alternatifleri sağlayarak ulaşım meselesini optimize edebilir.

Daha da önemlisi, artık ulaşım boyutunu daha geniş bir kentsel perspektifte düşünmek; duraklar, toplu taşıma saatleri, çalışanların çocuklarını bırakıp alabilecekleri çocuk bakım merkezleri, okullar vb. Hizmetlerin kullanımı gibi vatandaşların profesyonel ve kişisel yaşamları arasındaki etkileşimi daha iyi anlamaya çalışarak mümkündür. Örneğin, yüksek bir oranda vardiyalı çalışanı bulunan bir ilçe bu yöntemle çok daha iyi ulaşım sağlayabilir. Verilerin makul bir şekilde kullanılmasıyla, zorluklarla karşılaşan insanların yaşam koşullarını iyileştirmek mümkündür.

7.1.2. Veri Kullanımı ile İlgili Riskler

Veriler aslında kentsel sistemi nesnelleştirebilir, ancak sadece siyasi irade onu genel çıkar doğrultusunda yönlendirebilir. Bu da kurulan ortaklıkları anlamlandırır. Operatör, verilerin ekonomik ve teknik bilgisine sahiptir, ancak toplumun sosyal zekâsı da vardır. Düşünülmesi gereken yer de burasıdır. Başka bir deyişle, vatandaşlar, kamu otoriteleri ve ekonomik paydaşlar gibi şehrin bütün paydaşları bir araya gelerek bir şehri gerçekten akıllı yapabilir. Aksi takdirde, sadece mekanik veya ekonomik olacaktır.

Verilerin kullanımı ile ilgili temel riskler, gizlilik ve kişisel özgürlüklere saygı ilkelerine göre çerçevelenmelidir. Akıllı sayaçların örneği bu noktayı açık bir şekilde göstermektedir. Tüketimi izlemek, operatör için faturalandırmayı basitleştirir ve kullanıcı için kişiselleştirilmiş tüketim çözümleri sağlar. Ancak, tüketimin ölçüldüğü okuma sıklığı nihayetinde insanların yaşamlarının

mahremiyetini yani misafirlerinin olup olmadığı, gece boyunca düzenli olarak kalkılıp kalkılmadığı gibi bilgileri tespit ettiği için kişisel özgürlüğe saygı açısından bir risk oluşturur.

7.1.3. Veri Koruma ve İnovasyon Arasındaki Denge

Veri koruma ve yenilikçilik arasında adil bir denge bulunması esastır. Bu bağlamda karşımıza çıkabilecek ilk sorun sistemin varsayılan ayarlarını mümkün olduğunca dengeli olacak şekilde ayarlamamasıdır. Akıllı sayaçların okuma frekansı verilebilir. Okuma aralıkları düşük olan akıllı sayaçlar nedeniyle, operatörün, kullanıcının kişisel hayatını ayrıntılı olarak haritalayabilme riski doğmakta, yeterli ayrıntıyla tüketim miktarını izlemesini sağlamaktadır. Fakat çok büyük bir zaman aralığı verildiğinde de sayaçlar temel amacından saparak optimizasyon sağlayamaz duruma gelirler.

İkinci sorun ise; kişinin sistemin varsayılan ayarlarını değiştirme rızası olmadan değiştirilebilmesidir. Akıllı sayaç durumunda, okunan frekans kullanıcıdan izinsiz arttırılabilir. Benzer şekilde, kullanıcı rızası olmadan şirket tarafından erişilerek belli bir zaman aralığı boyunca verilerin yerel olarak depolanabilir.

Üçüncü ve sorun verilerin anonimliğidir. Farklı servisler arasında verilerin dolaşımına izin vermek son kullanıcıların gizliliğine zarar verebilir. Coğrafi konum örneğini ele alırsak bir bireyin coğrafi konum bilgisini bilmek, belirli sayıdaki şeyleri çıkarmaya yardımcı olabilir. Bir işverenin çalışanının her hareketini takip edip edemeyeceğini düşünürsek başka bir iş arama durumunda işverenin bunu anlaması kaçınılmazdır.

7.1.4. Diğer Yasal Problemler

Gizlilik sorunları dijital şehirlerdeki tek yasal sorun değildir. Öncelikle akıllı şehirlerin çalışması için gerekli olan verilerin, kamu makamları tarafından zorunlu olarak tutulup tutulmadığını anlamak önemlidir. Veriler; su, elektrik, gaz, ulaşım

veya park hizmetleri gibi yerel kamu sektöründe faaliyet gösteren şirketlerin hatta telekomünikasyon şirketleri gibi tamamen özel operatörlerin elinde olabilir. Dolayısıyla, "kamu yararı verileri" kavramının, kamu yetkililerine açık olması gerektiği fikri ortaya çıkmaktadır. Veri akışlarını eşleştirmek, verilerin kiminle temas noktası olduğunu, denetleyicinin ve işlemcinin kim olduğunu belirlemek ve uyumlu anlaşmalar yapılmasını sağlamak önemlidir. Bunlara ek olarak tüm halkın kullanımına açılacak olan açık veri, siber saldırganlar için bilgi toplama olanağı yaratabilir.

7.1.5. Yönetişim Faktörleri

Güvenlik konularını etkileyen ve tetikleyen bir diğer faktör olan yönetişim faktörleri; sağlık sektörü, altyapı, eğitim, ulaşım gibi konuları içermektedir. En büyük endişe, akıllı bir kentin tüm altyapı bakımı ve yönetiminin nasıl sağlanacağıdır.

Teknoloji şirketlerinin müşterileri olan yönetişim yetkilileri, satın aldıkları sistemlerin güvenliğini test etmek konusunda farkındalık sahibi değillerdir. (Why smart cities need to get wise, 2015) Öncelikleri, teknolojinin işlevselliğini test etmektir ve güvenlik testlerine odaklanılmaz. Yetkililerin güvenlik konularında bir kaygıya sahip olmamaları, doğabilecek çok büyük sorunların habercisidir. Çok basit güvenlik zafiyetlerinin çok büyük etkiler yaratabildikleri göz önüne alındığında, kritik bir sisteme gerçekleşen tek bir saldırı hizmetin gecikmesine veya kaybına yol açabilmektedir.(Abouzakhar, 2013) Ayrıca, kritik sistemler tarafından üretilen verilerin, düzgün bir şekilde depolanması, yönetilmesi ve korunması gerektiğinden veri bütünlüğü ve esnekliği konusunda büyük problemler doğabilir.(Symantec, 2010) En önemli kritik altyapı tiplerinden biri olan sağlık sektörü, sadece bir hastanın mahremiyet endişelerine neden olmakla kalmayıp, aynı zamanda kritik bilgilerin saldırgan tarafından değiştirilebilmesi nedeniyle hayatında tehdit dahi oluşturabilir. (Solanas, et al., 2014)

Veri toplama ve analiz etme sırasında bilgi ifşası meydana geldiği için akıllı mobil sistemlerde gizlilik problemleri oluşur. Burada lokalizasyon teknikleri GPS, GSM, Wi-Fi, Bluetooth ve RFID teknolojileridir. Akıllı telefon uygulamalarından bazıları, verileri küçük parçalara bölüp analiz etme ve veri madenciliği tekniklerini kullanır. Ayrıca, akıllı ulaşım altyapısında kullanılan cihazlardan alınan ve gönderilen veriler, uydu navigasyon sistemlerine gönderilen yanlış trafik raporları olarak kötü amaçlı saldırılar yapmak için kullanılabilir (Symantec, 2010). Bu nedenle, akıllı ulaşım alanındaki güvenlik ve gizlilik tehditlerini göz önünde bulundurarak bilgi ve haberleşme teknolojilerinin en iyi şekilde kullanılması gerekmektedir.

Enerji ve kamu hizmetleri, dağıtılmış enerjiyi verimli bir şekilde yönetmek için kullanıcılarla çift yönlü haberleşme kuran akıllı şebekelere giderek daha fazla önem vermektedir. Bulut bilişim akıllı şebeke yazılım platformları için uygun olan özellikleri sağlama konusunda önemli bir rol oynar. (Simmhan, Kumbhare, Cao, & Prasanna, 2011) Veri güvenliği ve gizlilik, kamu hizmetleri ve akıllı şebekelerin benimsenmesinde kullanıcılar için endişe konularıdır (Polonetsky & Wolf, 2009). Ayrıca, bulut sistemlerle uygulandığında sorunlar artmaktadır. Enerji ve kamu hizmetlerini dolandırıcılık ve kötü niyetli saldırılardan koruyabilmek için uygun bir strateji oluşturulmalıdır.

Günümüzde siber saldırılar bu kadar yaygınlaşmışken, birtakım önlemler alınmış olsa bile siber olay yaşanma olasılığı her zaman vardır. Bu durumlarda şehir yönetimi, bu saldırıların etkisini en aza indirgemekten ve şehrin işleyişinin sürdüğünden emin olmalıdır. Fakat şehirlerde siber olaylara müdahale ekiplerinin yetersizliği ya da bulunmaması, şehrin siber saldırılara karşı koymasını güçleştirebilmektedir. Siber saldırılara yeteri kadar hazırlıklı olmayan şehirlerin toparlanma süreci de bir o kadar uzun ve sancılı geçecektir.

7.1.6. Sosyal ve Ekonomik Faktörler

Akıllı bir şehirde, insanların sosyal problemleri yönetme talepleri; şehir planlaması, acil durum aksiyonları ve toplum yönetimi için akıllı şehri tek elden hizmet veren bir sisteme dönüştüren teknoloji ile karşılanır (Su, Li, & Fu, 2011). Akıllı bir şehir, bankacılık, finans ve iş faaliyetlerini daha verimli bir şekilde geliştirmek için hizmet sunduğundan daha akıllı ekonomik büyüme vaat eder. Akıllı bir şehirde sosyal ve ekonomik faktörler arasında iletişim, bireysel kimlik, bankacılık ve finans bulunmaktadır. Bunların hepsi akıllı bir şehrin kritik bir parçasıdır ve güvenlik ve gizlilik sorunlarına karşı savunmasızdır.

Telekomünikasyon sektörü, akıllı bir şehrin kritik altyapısının bir parçasıdır ve çeşitli zararlı saldırılara, virüslere, dolandırıcılıklara ve gizlilik saldırılarına karşı savunmasızdır. Çeşitli finansal ve yönetişim faaliyetleri telekomünikasyon ve kablosuz ağlar üzerinden gerçekleştirildiğinden güvenlik ve kimlik doğrulama ihtiyacı artmaktadır. Makineden makineye (M2M) haberleşme de aynı zamanda akıllı bir şehrin vatandaşlarına hizmet sunar (Wan, Li, Zou, & Zhou, 2012). Dolayısıyla M2M iletişimleriyle ilgili güvenlik tehditleri de dikkate alınmalıdır. Akıllı telefonların ve tabletlerin kullanımı, akıllı bir şehrin vatandaşları arasındaki iletişimine yeni ufuklar getirmiştir. Ayrıca, gizlilik ve bilgi güvenliği için de yeni tehditlere yol açmıştır. Bir teknoloji ne kadar yaygınsa saldırılara daha açık demektir. Akıllı telefonlar son yıllarda çok popüler hale geldiklerinden, saldırganların hedefi haline gelmiştir. Kablosuz ağ, bluetooth, bulut bilişim, IoT ve aslında hemen hemen tüm bilgi ve haberleşme teknolojileri akıllı haberleşmede rol oynar ve akıllı çözümler geliştirilirken bunlarla ilgili güvenlik kaygıları dikkate alınmalıdır.

Bankacılık, finans ve iş dünyası akıllı bir şehrin temel bir bileşeni olan akıllı ekonominin parçalarıdır. Akıllı şehirler ekonomide büyüme, daha iyi bankacılık ve ticari hizmetler için uğraş verse de akıllı bir şehrin bu bileşeni, kişilerin finansal kullanımlarına karşı saldırıya uğrayabileceğinden güvenlik tehditlerine karşı daha

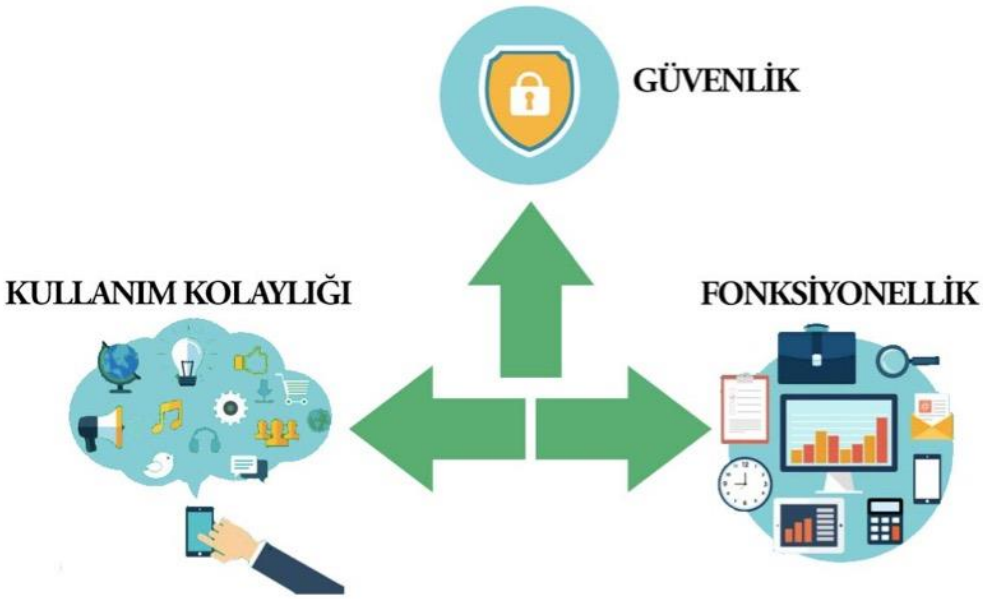
savunmasızdır. Saldırganlar ayrıca belli bir organizasyonun ekonomisini veya bütün bir şehri de sabote etmeyi amaçlar.

7.1.7. Teknolojik Faktörler

Teknoloji, akıllı bir kentin tüm vaatlerini yerine getirirken kilit rol oynar. Akıllı şehir, hükümete ve vatandaşlara daha iyi hizmet verebilmek için teknolojiye bağımlıdır. Akıllı şehir, bütünleşmiş ve güncel teknolojiyle daha akıllı ekonomik büyüme, daha akıllı yönetişim ve daha akıllı hizmetler vaat eder. Aslında akıllı şehirler güvenlik ve mahremiyetle ilgili kaygıların doğru bir şekilde karşılanmaması durumunda bu kadar akıllı değildir. Teknolojiden çok geniş bir ölçekte ve yoğun bir şekilde kullanılması, akıllı şehirleri kötü niyetli kişiler ve organizasyonların da hedefi haline getirmektedir.

Dünyanın dört bir yanındaki şehirler, güvenli olduğundan emin olmadan teknolojiyi kullanır. Henüz önemli saldırılar görülmemesine rağmen saldırganların şehirleri hedef alması an meselesidir. Akıllı şehir teknolojisini oluşturan ağların, on milyonlarca kullanıcı ve yüz milyonlarca cihaz ile birlikte bakımı, yönetilmesi ve kesintisiz hizmetinin sağlanması gerekliliği bulunmaktadır. Halihazırda sağlanması zor olan güvenlik gereksinimleri teknolojik altyapı genişledikçe saldırı yüzeyi arttığı için güvenliğin sağlanması da zorlaşacaktır.

Akıllı şehirler, kullandıkları teknolojilerle halkın yaşamını kolaylaştıracak çözümler sunar. Bu gereksinimin karşılanabilmesi sunulan çözümlerin fonksiyonel ve kullanışlı olması gerekir. Fakat bu iki metrik güvenlik ile ters orantılıdır. Daha fonksiyonel sistemler daha karmaşık altyapılar gerektirdiği için güvenliğin sağlanması zorlaşacaktır. Güvenlik işlemlerinin azaltılması ve güvenlik önlemlerinin gevşetilmesi hem servislere ekstra performans getirecek hem de kullanılabilirliği arttıracaktır. Fonksiyonelliğin artması da kullanılabilirliğin azalmasına sebep olmaktadır. Çok fazla fonksiyon sunan sistemlerin kullanımı zorlaşacaktır.



Şekil 18 Güvenlik, Kullanım Kolaylığı, Fonksiyonellik Üçgeni

Güvenliği ön planda tutacak akıllı şehirler, fonksiyonellik ve kullanım kolaylığından feragat edeceği için, akıllı şehir konseptinden uzaklaşmaya başlayacaktır. Akıllı şehrin güvenlik, kullanım kolaylığı ve fonksiyonellik üçgeninde kendine belirleyeceği yer güvenlik problemlerine sebep olabilir.

Akıllı şehirlerdeki teknolojik unsurların her biri sürekli olarak iletişim halindedir. Bu nedenle akıllı şehirlerdeki güvenlik problemlerinin teknolojik faktörlerini incelerken, nesnelerin interneti konseptinin güvenlik problemlerinden de bahsetmek gerekir. Büyük miktarda veri toplayan ve çok küçük cihazlarda dahil bağlantı özelliği bulunan nesnelerde hem toplanan verinin mahremiyetinin korunamaması hem de bu cihazların ele geçirilmesi riskleri bulunmaktadır.

İnternete sürekli bağlı halde çalışan nesneler her zaman uzaktan saldırıya açık haldedirler. Bir binada, bir evde birden fazla bağlı nesne olması saldırı yüzeyini daha da arttırmaktadır. Akıllı şehirler ise caddeleri, sokak lambaları, binaları, halka açık her türlü alanıyla internete bağlı sensörlerle doludur. Bu da saldırı yüzeyini devasa boyutlara çıkartmaktadır. Hayatımıza birçok fonksiyonellik sunan bu

cihazlar da diğer birçoğu gibi güvenlik gereksinimleri arka planda olarak üretilirler. Bu da akıllı şehirler için tehdidin daha da büyük olduğunu göstermektedir. Güvenlik araştırmacısı Cesar Cerrudo yaptığı çalışmada Washington DC, New York, Seattle, San Francisco 200,000 trafik kontrol sensörünün zafiyet içerdiğini gözlemlemiştir. (Cerrudo, 2014)

OWASP 'a göre 2014 Nesnelerin interneti konseptinde bulunan en yaygın on güvenlik zafiyeti yaygınlık oranına göre aşağıda listelenmiştir:

- Güvensiz Web Ara yüzü
- Yetersiz kimlik doğrulama/yetkilendirme
- Güvenli olmayan ağ servisleri
- Zayıf şifreleme kanallarının kullanımı
- Gizlilik endişeleri
- Güvensiz bulut ara yüzü
- Güvensiz mobil ara yüzü
- Yetersiz güvenlik yapılandırması
- Güvensiz yazılım/donanım yazılımı
- Yetersiz fiziksel güvenlik

Nesnelerin interneti konseptinde ciddi güvenlik problemlerine sebep olabilecek bir teknoloji de RFID teknolojisidir. Radyo frekansı tanımlama (RFID) etiketleri akıllı şehrin çeşitli bileşenlerinde çok fazla kullanılmaktadır. Gerçek zamanlı bilgi görünürlüğünü ve izlenebilirliğini geliştirerek birçok alanda da önemli faydalar sağlamıştır. RFID etiketleri, yetkisiz erişim yoluyla hassas bilgi ifşası, veri gizliliği ve veri bütünlüğünün bozulması gibi güvenlik problemleriyle karşılaşır. RFID etiketinin boyutu, maliyeti düşürecek kadar küçüktür. RFID etiketi çeşitli fonksiyonlara gömülebildiğinden güvenli koruma sistemi kurma marjı çok azdır. Şehirlerde kullanılan bu teknolojinin kullanımında karşılaşılabilecek başlıca problemler aşağıda listelenmiştir:

- Bu etiketler yetkisiz kullanıcılar tarafından yasa dışı kullanılabilir.

- RFID etiketi ve RFID okuyucusu arasındaki haberleşme, benzersiz bir Elektronik Ürün Kodu (EPC) aracılığıyla yapıldığından bu kod saldırgan tarafından ele geçirilebilir.
- Başka bir sorun etiketi sökmektir. Bu durumda RFID sistemindeki etiketli öğeleri tanımlayan uydu alıcı-vericileri, başka bir şeyle ilişkilendirilebilir ve etiketinden ayrılabilir.
- Etiketler, saldırgan tarafından silme veya öldürme komutlarının uygulanması veya fiziksel imha yoluyla kullanılamaz hale gelir (Mohite, Kulkarni, & Sutar, 2013). Sonuçta okuyucu etiketi tanımlayamaz veya okuyamaz. Etiket öldürme işleminin, gizlilik sorunlarını adresleyerek sistemin güvenliğini arttırmak için de kullanılabileceğini bilmek önemli bir noktadır.
- Etiket klonlaması, verileri orijinal bir etiketten alınması ve yakalanan verilerin yeni bir etikette izinsiz olarak kopyalanmasını sağlayan bir işlemdir. Kopyalanan veriler, saldırganın bir etiketine aktarılır.
- RFID için büyük güvenlik sorunlarından biri de okuyucunun istismar edilmesidir (Nie & Zhong, 2013). Eğer saldırgan RFID okuyucusunun kontrolünü ele geçirirse, RFID etiketindeki verileri yok etmek için bazı elektromanyetik dalgalar yayar.
- RFID etiketi, bir sistemin kullanıcılarının izni olmadan izlenebilir. Tanımlanan etiketlerin izlenmesi, sistemin kullanıcılarının özel bilgilerinin sızmasına neden olur. Yani etiket izleme bireysel gizliliğe zarar veren ana konudur (Aggarwal & Das, 2012).
- Bozma türündeki hizmet engelleme (Jamming Style DoS) saldırıları kasıtlı olarak radyo sinyali göndererek kablosuz iletim ortamındaki paketlerin bozulmasını ve böylece düğümler arasındaki iletişimin aksamasını ya da tamamen engellenmesini hedefleyen saldırı türüdür. Bu saldırı, güçlü vericiler tarafından önemli bir mesafede ve ekranlama (shielding) gibi pasif yollarla yapılır (Mohite, Kulkarni, & Sutar, 2013).
- RFID sisteminde okuyucular ve etiketler kablosuz iletişim kullanır. Kablosuz sinyallerin kullanılabilirliği, bir saldırganın kablosuz sinyalleri aramasını, değiştirmesini ve sinyalleri bozmasını kolaylaştırır. Böylece RFID okuyucuları

ve RFID etiketleri arasındaki kablosuz iletişimi korumak için şifreleme ve kimlik doğrulaması çok önemlidir.

- Yazılım saldırıları, işlevselliğini etkilemek için RFID sisteminde enjekte edilen virüsler, arabellek taşmaları (buffer overflows) ve solucanları (worms) içeren en bilinen saldırı türleridir. Bunlar, sistemi yavaşlatmayı veya yok etmeyi amaçlayan kodlanmış kötü amaçlı programlardır.
- Gizli dinleme (eavesdropping) ve kripto analiz RFID ataklarının en bilinenlerindendir. Ataklar ortadaki adam (man in the middle) saldırılarını da içerir.

Üçüncü bölümde de bahsedildiği gibi akıllı şehirlerde teknolojiden faydalanılan en önemli sektörlerden biri de enerji sektörüdür. Sürdürebilir ve verimli bir yaşam şansı sunan akıllı şehirlerde akıllı şebekeler ile enerji harcamaları optimize edilmeye çalışılmaktadır. Enerji dağıtımı ve yönetimi konusunda rol oynayan akıllı şebekeler inşa edilirken göz önünde bulundurulması gereken temel tehditleri aşağıdaki gibi sınıflandırabiliriz:

- Hizmet engellemesi (DoS) saldırıları, akıllı şebekedeki bilgileri kötüye kullanarak hizmetleri geciktirmeye, engellemeye veya bozmaya çalışır. Akıllı şebekeler çoğunlukla IP tabanlı protokolleri kullanır. TCP/IP, DoS saldırılarına açık olduğundan, bu tür saldırılar akıllı bir şebekede büyük sorun haline gelmektedir.
- Özellikle akıllı şebekelerde, sensör değerleri ve kontrol komutları gibi verilerde bütünlük önemlidir. Veri bütünlüğünün temel amacı, ağ üzerinde mesaj enjekte edilmesi, mesaj tekrarı ve mesaj gecikmesi gibi çeşitli yollarla veri değiştirme yöntemleri için savunma mekanizması olmaktır. Veri bütünlüğüne yönelik tehditler altyapıya veya insanlara zarar verebilir. Bütünlük saldırılarının ana amacı, müşteri bilgisi veya ağ operasyon bilgisidir. Bu saldırılar akıllı bir şebekede kritik verileri kötüye kullanma eğilimindedir. Yanlış veri (Rahman & Mohsenian-Rad, 2013) enjekte etme saldırıları ile veri bütünlüğünü bozmak için görüntüleme merkezine yanlış veriler gönderilir.

- Akıllı şebeke haberleşme sistemlerinin gizliliği, tüketicilerin temel endişesi ve hakkı olduğu için önemlidir. Akıllı şebeke iletişimi sırasında gerçek zamanlı olarak gizliliğe dikkat etmelidir.
- Akıllı sayaçlar; pil değişimi, sökülmesi ve modifikasyonu gibi fiziksel saldırılara maruz kalabilir.

Taşınabilirlikleri ve kullanım kolaylığıyla mobil cihazlar, insanları, akıllı şehirlerin teknoloji alt yapısına dahil eden araçlardır. Şehrin sunduğu çeşitli servisler bu kanal aracılığıyla ana hedef olan insanlara sağlanır. Mobil cihazlar son yıllarda oldukça popüler hale gelmiş ve saldırganlar tarafından ana hedeflerden birisi olmuştur. Akıllı cihazlardaki ana güvenlik tehditleri aşağıdaki gibi gösterilebilir:

- Popüler uygulamaları taklit eden uygulamalar uygulama pazarına yüklenebilir. Bu tür akıllı uygulamalar akıllı cihazlarına bulaşabilir ve birçok güvenlik ve bilgi gizliliği sorununa neden olabilir.
- Ele geçirilen cihazlar Botnet adı verilen uzaktan kontrol edilen cihaz ağlarına dahil edilebilir.
- Saldırganlar mevcut casus yazılımları kötüye kullanarak arama yapabilir, iletileri ve e-postaları kontrol edebilir veya GPS güncellemeleri aracılığıyla bir kullanıcı konumunu dahi izleyebilir.
- Son kullanıcıların bluetooth ayarlarını düzgün bir şekilde nasıl yöneteceklerini ve yapılandıracaklarını bilmedikleri durumlarda kablosuz cihazlar varlığını gösterir ve istenmeyen bağlantılara izin verir
- Akıllı telefonu ele geçiren saldırgan, akıllı telefonlar ve şehirdeki Wi-Fi hotspot'ları arasındaki haberleşme esnasında bilgi yakalayabilir.

Günümüzde yeni teknolojilerin çoğu kablosuz olarak çalışmaktadır. Şifreli olarak iletilmeyen kablosuz sinyaller yakalanabilerek dinlenebilmekte (eavesdropping), kesilerek kötü niyetli kullanıcılar tarafından değiştirilerek yönlendirilebilmektedir. Akıllı şehirlerde de iletişimin büyük bir bölümü kablosuz olarak

gerçekleştirilmektedir. Trafik ışıkları, kameralar, sokak lambaları, akıllı sensörler gibi cihazların birbirleriyle ve altyapıdaki sunucularla iletişimlerinin güvenli olarak iletilmesi önem arz etmektedir. Bu cihazların şifresiz olarak iletilmesi, kolay bir şekilde hacklenmelerine, veri sızıntısına veya kötü niyetli bir şekilde kullanılmalarına yol açabilir. Birçok cihaz, üreticiler tarafından düşük güvenlik önceliğiyle zayıf şifreleme algoritmaları kullanılarak üretilebildiği için bu konuda önlem alınması şarttır. Bazı durumlarda ise üreticiler tarafından güvenli şifreleme seçeneği kullanıcıya bırakılmasına rağmen, şehre entegrasyonu sırasında yanlış yapılandırma ile şehir içerisinde veri iletimi saldırıya açık bir konuma gelebilir.

Makineden makineye (M2M) haberleşmelerde bulabilecek güvenlik problemleri de akıllı şehir yaşamını olumsuz etkileyecektir. Makineden makineye protokoller, en az iki düğümü için olan bir ağdaki anlaşma kurallarını düzeltmek için kullanılır. İnternet Protokolü (IP) bu tür haberleşme amaçları için standart haline gelmiştir. İletişim için kullanılabilecek protokol örnekleri: ISA 100A, Link Katmanı, Kablosuz HART, IPv6 ve ZigBee. M2M iletişimlerinde ana güvenlik kaygıları:

- Fiziksel saldırılar, sahtekârlık amacıyla değiştirilmiş yazılımları kullanır. Ana ihlaller genellikle veri bütünlüğü ve M2M yazılımlarındadır.
- Kimlik doğrulama token'ları kötü amaçlar için kopyalanabilmektedir.
- Ortadaki adam (Man In The Middle) ve DoS saldırıları gibi protokol saldırıları riski oluşabilmektedir.
- Ağ güvenliğindeki tehditlerde esas olarak mobil ağlar hedeflenir. Bu tür tehditlere örnek olarak, aygıtların kimliğine bürünme ve bunlar arasında trafik tüneli oluşturma vardır. Ayrıca, güvenlik duvarının yanlış yapılandırılması da ciddi bir ağ güvenliği ihlalidir. Ağdaki DoS saldırıları da büyük bir sorun teşkil eder.
- M2M haberleşmesi esnasında veri toplama, veri madenciliği gibi işlemler yapılabilmektedir.

Şeklinde sıralanabilir. (Hongsong, Zhongchuan, & Dongyan, 2011)

7.2. AKILLI ŞEHİR YAPILANMASINDA TAKİP EDİLMESİ GEREKEN PRENSİPLER

Her sistemde olduğu gibi akıllı şehirlerde siber güvenlik stratejisi oluştururken dikkat edilmesi gereken temel prensipler vardır:

- *Gizlilik:* Dijital bir yaşam alanı olan akıllı şehirlerde, kullanılan verilerin gizliliği sağlanmalıdır. Birbirleriyle sürekli haberleşme durumunda olan cihazların iletişimin farklı kişiler tarafından da dinlenemediğinden emin olunmalıdır.
- *Doğru hedeflere odaklanma:* Akıllı şehre karşı oluşan tehditler titizlikle analiz edilmelidir. Şehrin ne tür tehditlere karşı olduğu bilinmediğinde şehir saldırılara karşı daha kırılgan bir yapıya sahip olacaktır. Tehditlerle birlikte şehrin ne gibi zafiyetlere sahip olduğu bilinmeli ve bunlara karşı doğru önlemler alınmalıdır.
- *Katılım:* Katılım prensibi, şehirleri akıllı yapan faktörlerden biri olduğu gibi, aynı zamanda güvenliğin sağlanması konusunda da önem taşımaktadır. Siber güvenliğin sağlanması sürecinde her paydaşın katılımı önem taşımaktadır.
- *Şeffaflık:* Siber güvenlik önlemlerini alan servis sağlayıcıların ve yönetimlerin şeffaflığı, karşılıklı güven ortamı oluşması ve acil durumlarda daha hızlı aksiyon alınması konusunda önemlidir.
- *Düşük risk:* Akıllı şehirlerde siber güvenlik önlemleri alınırken amaç doğacak riski düşürmek olmalıdır. Daha önce belirtildiği gibi risk formülündeki Siber saldırı olasılığı ve saldırıların olası etkisi azaltıcı önlemler alınmalıdır.
- *Saldırı yüzeyinin minimize edilmesi:* Bir bütün olarak akıllı şehirler büyük bir saldırı yüzeyi teşkil etmektedir. Bu prensibe göre saldırganların belli bir sistemde veya cihazda bulduğu güvenlik açıklığının, diğer sistemleri de risk altına atması engellenmelidir.
- *Derinlemesine güvenlik:* Güvenlik kontrollerinin katmanlandırılarak güvenliğe derinlik katılması ve saldırıların başarı şansını düşürme prensibidir. Bu prensiple birlikte sadece tek bir katmanı atlatan saldırgan asıl amacına ulaşamayacak, görülecek hasar azalacak, saldırıya karşı alınacak aksiyon için zaman kazanılacaktır.

- *Beyaz liste:* Bu prensibe göre belirli bir hizmet veya erişim sadece önceden belirli kişilere verilmelidir. Kullanıcılardan sistemlere gelen girdilerin kontrolünde de bu prensip rehber alınmalıdır.
- *Minimal yetki:* Bu prensibe göre kullanıcılara verilecek yetkilendirme, gerçekleştirecekleri işlemleri yerine getirecek kadarından fazla olmamalıdır.
- *Bilinmezlikle güvenlikten kaçınma:* Literatürde "avoiding security by obscurity" olarak bilinen bu prensip, akıllı şehirler için de takip edilmelidir. Bu prensibe göre, güvenlik, belirli detaylar gizli tutularak sağlanamaz.
- *Görevlerin ayrılığı ilkesi:* Bir görevin, farklı yetkiler tanımlanarak farklı kişilere bölünmesidir. Genel olarak çıkar çatışması ve sahtekarlığın önüne geçmek için takip edilmektedir. Örnek olarak izleme ve test etme, denetim ve raporlama farklı kişi ve kişilerce yapılması görevler ayrılığı ilkelerine uygundur.
- *Farkındalık:* Güvenlik bakış açısından, sistemlerin en zayıf halkası insanlardır. Kullanılan donanım veya yazılımlarda bilinen zafiyetler olmasa bile yapılacak insan hataları, saldırganlar için giriş kapısı oluşturmaktadır. Odak noktası insan olan ve insanlar tarafından yoğun olarak kullanılacak olan akıllı şehrin teknolojik alt yapısı aynı zamanda insanlar tarafından yönetilecektir. Bu prensip gereği teknolojiyle etkileşim içerisinde olacak insanların, durum ve olaylara güvenlik farkındalığıyla yaklaşması gerekmektedir.
- *Değişime açık olma:* Sürekli bir değişim içerisinde olan dünyada, kullanılan teknolojiler de sürekli olarak değişim halindedir. Değişen sistemlerin mevcut altyapıya entegrasyonu, güvenlik bakış açısıyla gerçekleştirilmeli ve kötü niyetli kullanıcılar için giriş kapısı olması engellenmelidir.
- *Yedekleme ve loglama:* Sistemlerin her an bir sistem hatası veya siber saldırıdan etkilenebileceği göz önünde bulundurularak düzenli olarak yedekleme yapılmalı ve kurtarma planları oluşturulmalıdır. Ayrıca olası bir saldırı sonrası durum için loglama yapılmalıdır.

7.3. AKILLI ŞEHİR YAPILANMASINDA ALINACAK ÖNLEMLER

Akıllı şehirlerde karşılaşılacak siber güvenlik problemleri ve siber saldırı senaryoları bölümlerinde de örneklerle anlatıldığı gibi akıllı şehirler, saldırganlar için geniş bir saldırı yüzeyi teşkil etmektedir. Sahip olduğu kaynak ve imkanlarla da kötü niyetli kişi ve örgütler için çekici bir hal alan akıllı şehirlerde yaşanacak bir siber olay, şehir yaşantısını sekteye uğratacak, şehirdeki tüm canlıların yaşamları olumsuz etkilenecektir. Bu nedenle akıllı şehirlerde siber güvenliğe gereken önemin gösterilmesi elzemdir. Hayati önem taşıyan siber güvenlik, akıllı şehirlerin dizaynı esnasında göz önüne alınmalı ve sistemler henüz kurulmadan önce güvenlik bakış açısıyla yaklaşılmalı ve güvenli bir mimari üzerine oturtulmalıdır.

7.3.1. Geleneksel Çözümler

Teoride mümkün olsa da pratikte yüzde yüz güvenlik mümkün değildir. Akıllı şehirler yapıları gereği, güvenlik, kullanım kolaylığı ve fonksiyonellik üçgeninde her üç bileşenden de vazgeçemeyecek bir konumdadır. Bu nedenle bu üçgendeki konum iyi belirlenmelidir.

Akıllı şehirlerde kullanılan teknoloji altyapısı ile ilgili bir önceki başlıkta anlatılan prensipleri takip edilerek saldırı yüzeyinin minimum olduğu, saldırı durumunda geri dönüşün mümkün ve çabuk olduğu sistemler kurulmalıdır.

Akıllı şehirlerde Makineden makineye (M2M) güvenli veri iletimi sağlamak için çeşitli çözümleri vardır. IEEE, akıllı bir şehrin uygulanmasında yararlı olan fiziksel (PHY) ve ortam erişim kontrolü (MAC) katmanları için standart mekanizmalar sağlamaktadır.

Akıllı şehirlerde güvenlik için dikkat edilmesi gereken bir diğer konu da erişim kontrolüdür. Erişim kontrolünde alınacak önlemler fiziksel ve mantıksal olarak iki ana bölümde incelenebilir.

Fiziksel erişim kontrolü önlemleri, kritik sistem ve verilerin bulunduğu odalar, binalar ve şehrin her türlü fiziksel cihazına fiziksel erişimin kısıtlanması için alınan önlemlemlerdir.

Mantıksal erişim kontrolü ise bilgisayar ağlarına, dijital dosya sistemleri ve verilere uzaktan erişim sınırlandırması getirmeyi amaçlamaktadır. Mantıksal erişim kontrolleri, kimlik doğrulama, yetkilendirme adımlarını içerir. Multi faktör kimlik doğrulama mantıksal bir erişim kontrolüdür ve üç ana faktör olarak incelenir. Bazı durumlarda konum ve zaman bilgisi de dördüncü ve beşinci faktör olarak değerlendirilebilir. Bilgi faktörü, kullanıcının bildiği ve sunucuların veri tabanında bulunan bir bilgiyi sunmasını ister. Buna örnek olarak PIN kodu, kullanıcı adı, parola, gizli soru ve cevabı verilebilir.

Bir diğer faktör mülk faktörüdür. Bu faktöre göre kişinin kimlik doğrulaması sahip olduğu bir cihaz kontrol edilerek gerçekleşir. Buna örnek olarak token üreticiler, sahip olunan mobil cihazlar verilebilir.

Üçüncü faktör ise genetik faktörlerle kimlik doğrulamadır. Kullanıcıların parmak izi, iris gibi biyolojik özellikleri kullanılır.

Saldırganların sistemlere girişte kullandığı en yaygın yöntemlerden birisi bilinen zafiyetleri bulunan ürünlerin istismar edilmesidir. Bu nedenle yama ve ayarların yönetilmesi ve kontrolü, alınması gereken en önemli önlemlerden biridir. Fakat akıllı şehirler gibi karmaşık ve büyük sistemlere sahip şehirlerde yama yönetimi çok zorlaşabildiği göz önünde bulundurulmalıdır.

Saldırganların kullandığı bir diğer yaygın giriş yöntemi de düzgün konfigüre edilmemiş ürünlerdir. Yanlış konfigüre edilen ürünler, saldırganların sistem üzerinde kabuk çalıştırmasına veya hak yükseltmelerine sebep verilebilir. Bu

nedenle kullanılacak yazılım ve donanımların doğru bir şekilde ve güvenlik bakış açısıyla konfigüre edilmiş olduğundan emin olunmalıdır.

Akıllı şehirlerde yaşanacak herhangi bir aksaklık şehirde yaşayanlara ve ekonomiye büyük zararlar verebilir. Bu nedenle sistemlerin sürekli olarak fonksiyonelliğinin korunduğundan emin olunacak önlemler alınmalıdır.

Siber güvenlikteki en zayıf halka ilk günden beri insandır. Bu nedenle insanlara güvenlik farkındalığı kazandırmak da alınması gereken önlemlerden bir tanesidir.

7.3.2. Yasal Çözümler

Alınacak geleneksel çözümler tek başlarına yeterli olmayacağı gibi yaptırımları da yasal bir zorlama ve denetim olmadığı durumlarda ihmal edilebilir.

Çıkartılacak yasalarda toplanan verilerin gizliliğini koruyamayan veya güvensiz ürünleriyle şehir işleyişine zarar her bir aktörün siber suçlular kadar suçlu olduğu unutulmamalıdır.

Yönetimler, çıkaracakları yasalarla veya mevcut yasaların yürürlüğünün denetimiyle siber suçların da çekiciliğini azaltmak durumundadır. Siber suçlular, gerektiği şekilde cezalandırılmalıdır.

7.3.3. Modern Çözümler ve Ar-Ge

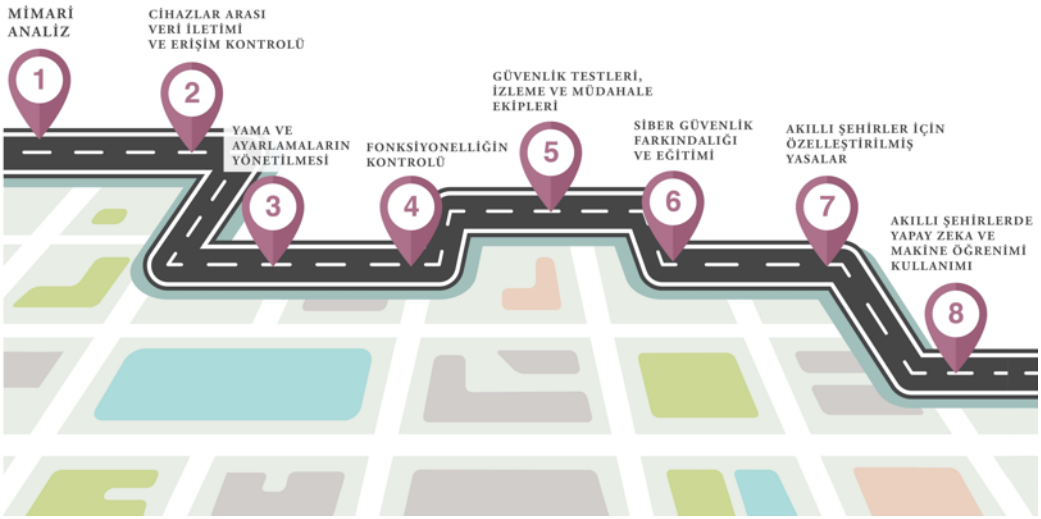
Yapay zekâ ve makine öğrenimi gibi bilgisayar bilimi dalları hayatımızın her alanında olduğu gibi akıllı şehirlerde de çok önemli yer tutacaklardır. Akıllı şehir servislerinde kullanılan bu teknolojiler, siber güvenlik çözümlerine de uygulanabilir. Saldırı mekanizmalarının her geçen gün daha ileri seviyelere geldiği siber uzayda, güvenlik çözümlerinde de yenilikçi olunması zorunlu hale gelmiştir. Yapay zekâ ve makine öğrenimi çözümlerinin kullanım alanlarına göre yüzdeleri aşağıda listelenmiştir (Oltsik, 2018):

- %29 Olay tespit sürecinin hızlandırılması
- %27 Olay yanıt sürecinin hızlandırılması
- %24 İş riskinin tespit edilmesi
- %22 Durumsal farkındalığın arttırılması

Şu an genel olarak dünya üzerinde yaygın olmasa bile girişimciliğin ön planda olduğu akıllı şehirler bu konuda da öncü olabilir. Hem hazır teknolojilerin şehre entegre edilmesi hem de Ar-Ge çalışmalarıyla yeni teknolojiler üretilmesi düşünülebilir.

SEKİZİNCİ BÖLÜM

AKILLI ŞEHİRLERDE SİBER GÜVENLİK YOL HARİTASI ÖNERİSİ

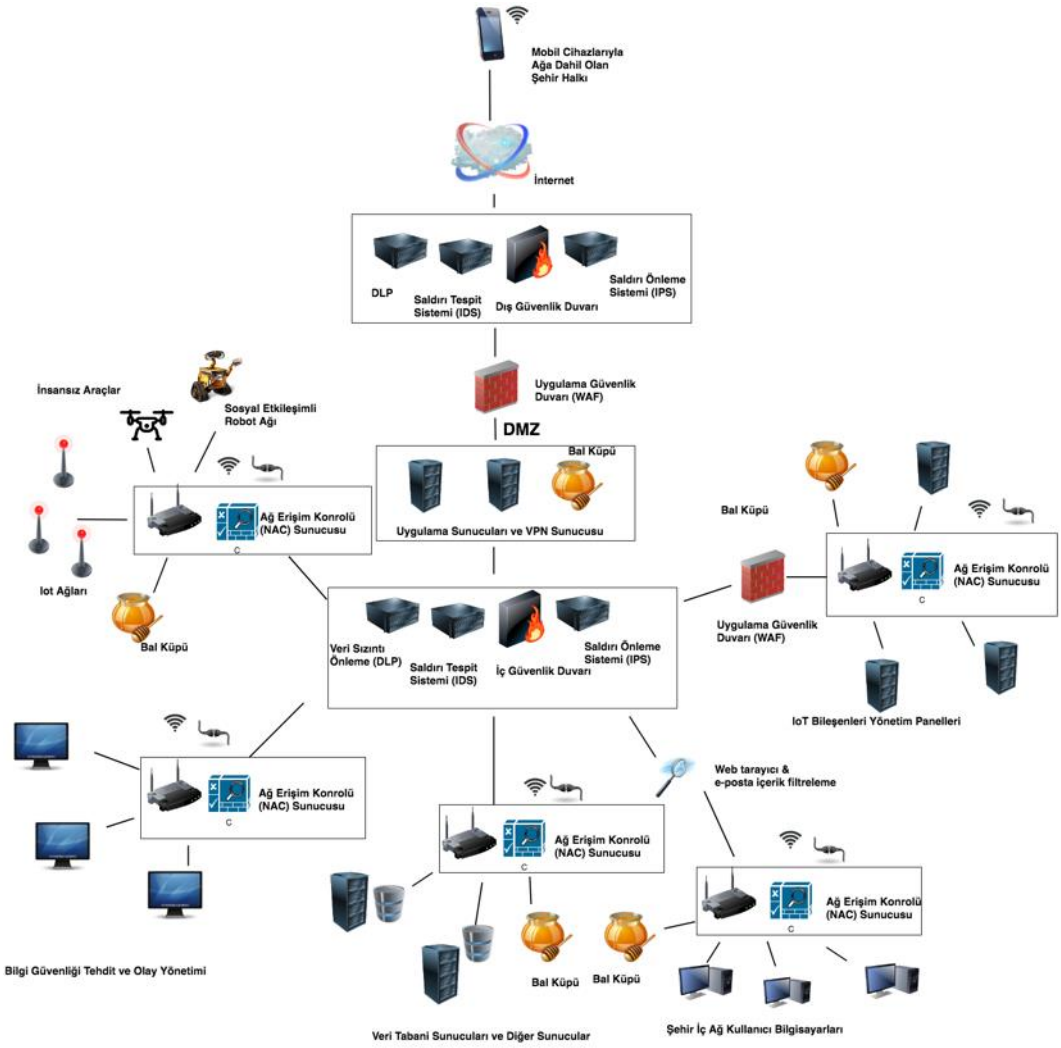


Şekil 19 Akıllı Şehirlerde Siber Güvenlik Yol Haritası Önerisi

8.1. MİMARİ ANALİZ

Akıllı şehirlerde sistemler oluşturulurken veya sisteme yeni parçalar eklenirken, saldırı yüzeyi olabildiğince küçük tutulmalıdır. Bu nedenle ağlar arasındaki izolasyon iyi sağlanmalıdır. Örnek olarak, 3 boyutlu yazıcı ağına bir şekilde dahil olan bir saldırgan, kritik verilerin depolandığı veri tabanlarına erişememelidir. Aynı zamanda, aynı ağ üzerinde bulunan bağlı cihazlar arasında zayıflık bulunduran bir cihaz bulunmadığından da emin olunmalıdır.

Güvenli ve güvensiz kaynaklar birbirlerinden ayrı tutulmalıdır. Askerden arındırılmış bölge (DMZ) yapıları düzgün bir şekilde konfigüre edilerek kurulmalıdır.



Şekil 20 Güvenli Akıllı Şehir Topolojisi

Kullanılacak uygulamalar da dizayn aşamasında güvenli mimariler üzerine inşa edilmelidir. Örneğin kullanıcı girdilerinin kontrolü ve sanitizasyonu, uygulamanın alacağı her girdi için beyaz liste yaklaşımıyla eksiksiz bir şekilde yapılmalıdır.

8.2. CİHAZLAR ARASI VERİ İLETİMİ VE ERİŞİM KONTROLÜ

Akıllı bir şehir için düşük güç ve kısa menzilli IoT operasyonları için üç temel güvenli protokol temel alınmalıdır (Bai, Xue, & Wang, 2012):

- IEEE 802.15.4 ZigBee

- IEEE 802.15.1 Bluetooth
- IEEE 802.11i WPA2

Mobil cihazlarda veri iletimi içinde kullanılacak güvenli protokoller aşağıda listelenmiştir:

- ETSI M2M
- 3GPP LTE-M

Ayrıca mobil cihazlar için geliştirilen akıllı şehir uygulamaları için kullanılacak API'ler de işlevselliklerini güvenli olarak sürdürebilmeleri için gerekli kriptografik özelliklere sahip olmalıdırlar.

Fiziksel güvenlikte de derinlemesine savunma prensibi takip edilmelidir. Alınacak fiziksel erişim kontrolü önlemleri aşağıda listelenmiştir:

- Şehrin her bir noktası kameralar ile izlenmeli, şehirdeki araçlar üzerlerindeki RFID etiketleriyle takip edilmelidir. Bu işlemlerde gizliliğin sağlandığından emin olunmalıdır.
- Kritik önem taşıyan sistemlerin bulunduğu alanların en dış kısmı için parmaklıklı duvarlar, dikenli teller konulabilir araç girişlerinin kontrolü için fiziksel engeller ve tuzaklar yerleştirilebilir.
- Değerli varlıklar kilitlerle korunmalıdır. Anahtarlar sadece yetkili kişilerde bulunmalıdır. İkinci bir faktör güvenlik önlemi için biyometrik kontrol konulabilir.
- Şehir içerisinde aydınlatmanın düzgün yapılması gerekmektedir.
- Sensörlerle birlikte şüpheli hareket tespiti yapılmalı ve alarm üretilmesi sağlanmalıdır.
- Kritik sistemlerin bulunduğu odalar için duman ve yangın dedektörleri eklenmelidir.
- Bina ve odalara giriş kontrolü akıllı kartlar ve/veya biyometrik kontroller ile sadece yetkili kişilerce gerçekleştirilmelidir.
- En önemlisi de kritik varlıklar, herkesin kolaylıkla erişebileceği noktalarda bulunmamalıdır.

Mantıksal erişim kontrollerinin kimlik doğrulama konusunda da derinlemesine savunma prensibi uygulanarak erişim için multi faktörlü kimlik doğrulama uygulanmalıdır. Özellikle bilgi faktörü için akıllı şehirlerde kullanılacak parolaların uzunluğuna ve karmaşıklığına dikkat edilmeli, aynı zamanda parolalar veri tabanlarına tuzlu hashler olarak depolanmalıdır. Hash algoritmasının MD5 gibi zayıf algoritmalar olmaması önemlidir. Genetik faktörü kullanılacak ise, kullanılacak algoritmaların false positive ve false negative olasılıkları minimum olmalıdır.

Şekil 21 Multi Faktörlü Kimlik Doğrulama Uygulanması

Güvenlik duvarları da erişim kontrolleri için akıllı şehir altyapılarında kullanılmalıdır. Yapılandırılacak güvenlik duvarlarında dikkat edilmesi gereken en önemli nokta konfigürasyon ve kural setleridir. Güvenlik duvarlarının yanında kritik sistemler için IDS, IPS gibi izinsiz giriş (intrusion) tespit ve engelleme yapan cihazlarla Honeypot (Balküpü) gibi tuzaklarla yetkisiz erişim tespitleri yapılmalıdır. Fakat, güvenlik duvarları, IDS, IPS gibi cihazların tek başlarına hiçbir zaman güvenlik için yeterli olmadığı da unutulmamalıdır.

Akıllı şehirlerde kimlik doğrulaması, kritik sistemler ve uygulamalar için çok faktörlü, diğer sistemler için minimum bir faktör olacak şekilde gerçekleştirilmelidir.

Kimlik doğrulama gerçekleştirildikten sonra yetkilendirme adımı gerçekleşmelidir. Sistemlerde bulunan kullanıcı hesaplarının yetkilendirmesi titizlikle yapılmalı ve minimal yetki prensibiyle hareket edilmelidir. Kullanıcıların yetkilerinden daha fazla işlem yapamadığından ve aynı zamanda bir lokal admin hesabının diğer sistemlerde de yetkili olmadığından da emin olunmalıdır.

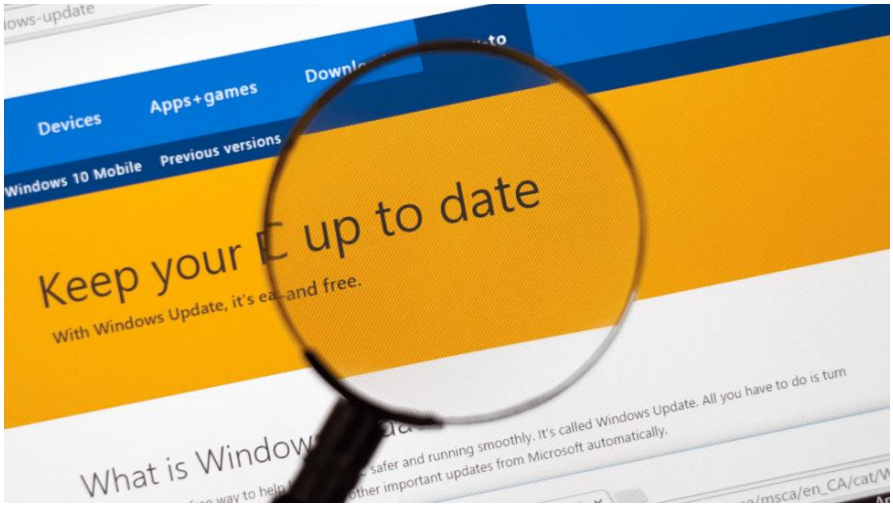
Bu konuda alınması gereken son önlem loglamadır. Sistemlere erişimler ve yapılan işlemlerin logları tutulmalıdır. Alınan logların kişisel verileri ortaya çıkartmadığından emin olunmalıdır.

8.3. YAMA VE YAPILANDIRMALARIN YÖNETİLMESİ

Akıllı şehirlerde kullanılacak teknoloji altyapısında her bir ürünün güncel olduğundan emin olunmalıdır. Yamalar geçilmeden önce test ortamında test edilip, sistemin işleyişine etkisi olmadığından emin olunduktan sonra geçilmelidir. Bu durumlarda risklerin öncelikleri belirlenmeli ve vakit kaybetmeden yamalar geçilmelidir. Özellikle imza tabanlı çalışan IDS, anti virüs gibi güvenlik ürünlerinin de sürekli olarak güncellendiğinden emin olunmalıdır.

Akıllı şehirlerde kullanılacak donanım ve yazılımların doğru konfigüre edilerek, güvenlik riski oluşturması engellenmelidir. Bu nedenle kurulan ürünlerin otomatik taramalarla ve hizmet sağlayıcı desteğiyle düzgün kurulduğundan emin olunmalıdır. Ayrıca sistemlere düzenli olarak kontrollü bir şekilde sızma testi gerçekleştirilmesi, yanlış ayarlamaların ortaya çıkartılmasındaki en etkili yöntemlerden bir tanesidir.

Yama ve ayarların yönetilmesinde, sistem yöneticilerinin ve normal kullanıcıların güvenlik farkındalığı seviyeleri önem taşımaktadır.



Şekil 22 Yamalar

(Navarro, 2017)

8.4. FONKSİYONELLİĞİN KONTROLÜ

Akıllı şehirlerde fonksiyonelliğin korunduğu kontrol edilmeli aksi durumlarda alarmlar üretilerek hızlı bir şekilde aksiyon alınması sağlanmalıdır. Kullanılan yazılım ve donanımlar, beklenmeyen durumlarda alarm üretecek şekilde yapılandırılmalıdır. Kullanılmayan ve gerek olmayan servisler kapatılmalıdır.

Şehirde depolanan kritik verilerin yedeklendiğinden emin olunmalıdır. Yedekler de asıl veriler gibi güvenli bir şekilde saklanmalıdır. Aynı zamanda herhangi bir hizmet kesintisi veya bozulma durumunda kullanılacak imajlar, yedek donanımlar ve jeneratörler de bulundurulmalıdır.

Şekil 23 Fonksiyonellik

(D'Agostino, 2018)

8.5. GÜVENLİK TESTLERİ, İZLEME VE MÜDAHALE EKİPLERİ

Akıllı şehirlerde kurulacak ve hazır sistemlerin sürekli olarak otomatik ve manuel olarak test edilmesi, izlenmesi ve acil durumlarda en kısa zamanda müdahale edilmesi gerekmektedir. Fakat genellikle şehirler için özel olarak çalışan güvenlik ekipleri bulunmamaktadır.

Akıllı şehir güvenlik yol haritası kapsamında, şehirlere özel olarak güvenlik ekipleri kurulmalıdır. Ayrıca olası bir siber saldırıya karşı anında müdahale edebilecek, zafiyet raporlaması, güncellemesi ve 7/24 izleme gerçekleştirecek bir SOME (Siber olaylara müdahale ekibi) kurulması da gerekmektedir.

Güvenlikte bir ikinci gözün de kontrolü önemli olduğundan güvenilir firmalardan ekstra destek de alınması önerilir. Sistemler düzenli olarak manuel kontrollerin yanında otomatik araçlarla güvenlik zafiyetlerine karşı taranmalıdır.

Şekil 24 Siber Olaylara Müdahale Ekibi

(Moonshinenews, 2016)

8.6. SİBER GÜVENLİK FARKINDALIĞI VE EĞİTİMİ

Akıllı şehirde yaşayan her bir insanın güvenlik farkındalık seviyesinin istenen seviyeye gelmesini sağlayacak eğitimler, afişler ve konferanslar düzenlenmelidir. Aynı zamanda ilkokul veya orta okul seviyesinden başlayarak siber uzay ve güvenlik gibi kavramlara aşinalık kazandırılarak, siber saldırılara karşı bütün insanların bilinç kazanması sağlanmalıdır.

Kalifiye güvenlik personeli yetiştirilmesi için üniversitelerde siber güvenlik programlarının açılmalı, teşvik edilmeli ve yetenekli insanlar bu alana yönlendirilmelidir.

Şekil 25 Siber Güvenlik Farkındalığı

(UBC, 2017)

8.7. AKILLI ŞEHİRLER İÇİN ÖZELLEŞTİRİLMİŞ YASALAR

Akıllı şehirler tarafından çıkartılacak şehir yasalarıyla hem kamu hem özel sektörün, güvenliğe zorunlu yatırımlar yapması teşvik edilmeli, denetlenmeli, uyumluluk sağlamayanlar cezalandırılmalıdır.

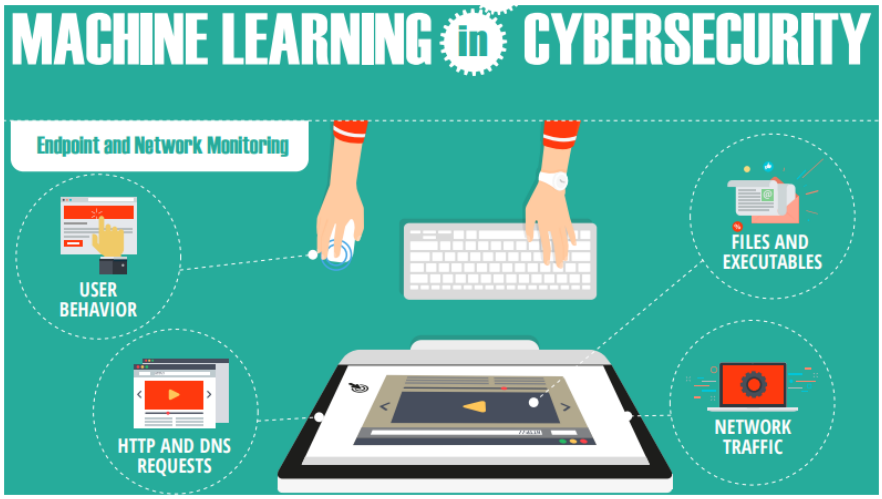
Ayrıca çıkartılacak yasalarla, yazılım veya donanım üreten şirketlerin, güvenli dizayn prensibini benimsemeleri, her türlü şirketin düzenli olarak güvenlik testi yaptırmaları yasal zorunluluk haline getirilmelidir.

Şekil 26 Siber Yasalar

(Egan, 2017)

8.8. AKILLI ŞEHİRLERDE YAPAY ZEKA VE MAKİNE ÖĞRENİMİ KULLANIMI

Akıllı şehirlerde, yapay zeka ile çalışan ve çeşitli makine öğrenimi algoritmalarını kullanan özellikle IPS, IDS gibi cihaz ve programlar, geleneksel çözümleri tamamlayıcı unsurlar olarak kullanılmalıdır. Bunun yanında şehirdeki üniversiteler ve Ar-Ge yapan şirketler, bu tip yenilikçi güvenlik araştırmaları ve ürün geliştirme konusunda teşvik edilmelidir.



Şekil 27 Siber Güvenlikte Makine Öğrenimi

(Jamalpur, 2017)

SONUÇ

Günümüzde teknoloji çok hızlı bir şekilde ilerlemekte ve hayatlarımıza entegre olmaktadır. Daha önce evlere girmesi beklenmeyen bilgisayarlar artık her insanın ceplerine girmiştir. İnternetin yaygınlaşması ve çevremizdeki birçok cihaza işlem gücü kazandırılmasıyla birlikte nesnelerin interneti konsepti gündeme gelmiştir. İnternet üzerinden birbirleriyle aynı olan cihazlar birçok veri toplayıp işlemekte ve ağ üzerinden iletimini sağlamaktadır.

İnsanların yaşadığı şehirler de teknolojinin gelişiminden etkilenmiştir. Daha yaşanılabilir, verimli ve sürdürülebilir şehirler için teknolojiden faydalanılmış ve akıllı şehir kavramı ortaya çıkmıştır. Mobil cihazlar ve dijital platformların git gide yaygınlaşması, toplanan verilerle birlikte çıkan büyük veri ve açık veri kavramları o, nesnelerin interneti konsepti, üç boyutlu yazıcılar, sosyal etkileşimli robotlar ve insansız araçlarla birlikte akıllı şehirler, her unsuru bir ağa bağlı yapılar haline gelmiştir. Her bir cihazın ve insanın bu geniş ağ üzerinde bulunması akıllı şehirleri siber saldırıların da hedef noktası haline getirmiştir.

İnsanların yaşamını kolaylaştırmayı amaçlayan akıllı şehirlerin siber saldırılarla birlikte işlevsiz hale gelmesi, kritik verilerin sızması, kaynakların yok olması gibi olasılıklar mevcuttur. Bu gibi durumlarda akıllı şehir olmaktan uzaklaşacak olan şehirlerde siber saldırı olasılığı ve olası etkileri ile artan siber risk, en düşük seviyede tutulmalıdır. Siber riskin minimize edilmesi, sadece teknolojik ürünlerdeki zafiyetlerin kapatılmasıyla mümkün değildir. Kamu kuruluşları, özel şirketler, şehir yönetimleri ve şehir sakinleri, siber güvenliği bir araç değil bir amaç olarak benimsemek durumundadır.

Siber güvenliğin sağlanabilmesi için çeşitli güvenlik prensipleri takip edilerek önlemler alınmalıdır. Alınacak önlemler; veri iletiminin şifrelenmesi, yama ve ayarların yönetilmesi, güvenlik testi, izleme ve müdahale ekipleri kurulması gibi geleneksel önlemler, çıkarılacak yasalarla güvenliğin öneminin vurgulanması ve güvenli teknolojiler üretilmesi gibi yasal çözümlerle ve yapay zeka ve makine

öğrenimi gibi teknolojilerden faydalanan ürünler gibi modern çözümler şeklinde gruplandırılabilir.

İnsanların yaşam merkezi olacak akıllı şehirler kurulurken, güvenlik bakış açısıyla tasarlanmalı ve siber riski minimum seviyeye düşürecek önlemler alınmalıdır. Her türlü kurumun, devletin veya insanın başına gelebilecek siber saldırıların, akıllı şehirler tarafından en kısa zamanda ve en az kayıpla savuşturulması amaçlanmalıdır.

REFERANSLAR

Abouzakhar, N. (2013). Critical infrastructure cybersecurity: A review of recent threats and violations.

Aggarwal, R., & Das, M. L. (2012). RFID security in the context of "internet of things". *Proceedings of the First International Conference on Security of Internet of Things - SecurIT 12*. doi:10.1145/2490428.2490435

Aldairi, A., & Tawalbeh, L. (2017). Cyber Security Attacks on Smart Cities and Associated Mobile Technologies. *Procedia Computer Science*, *109* (2016), 1086–1091. https://doi.org/10.1016/j.procs.2017.05.391

Bai, S., Xue, Z., & Wang, Y. (2012). Research on security of wpa/wpa2 protocol. *Information Security and Communications Privacy*, *1*, 106-108.

Car sharing Copenhagen, Aarhus, and Odense. (n.d.). Erişim: 09 Nisan 2018, https://letsgo.dk/en/

Cerrudo, C. (2014). Hacking US (and UK, Australia, France, etc.) Traffic Control Systems. Erişim: 18 Nisan 2018, http://blog.ioactive.com/2014/04/hacking-us-and-uk-australia-france-etc.html

Cerrudo, C. (2015). Why smart cities need to get wise to security and fast. Erişim: 14 Nisan 2018, https://www.theguardian.com/technology/2015/may/13/smart-cities-internet-things-security-cesar-cerrudo-ioactive-labs.

City of Copenhagen. (2015). CPH 2025 Climate Plan, A Green, Smart and Carbon Neutral City. Erişim: 10 Nisan 2018, http://kk.sites.itera.dk/apps/kk_pub2/pdf/983_jkP0ekKMyD.pdf

City of Copenhagen. (2015). The City of Copenhagen's Business and Growth Policy, 1–24. Erişim: 9 Nisan 2018,

https://international.kk.dk/sites/international.kk.dk/files/uploaded-files/Business_and_%20Growth_%20Policy.pdf

CNBC. (2018). Facebook-Cambridge Analytica: A timeline of the data hijacking scandal. Erişim: 21 Haziran 2018, https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html

Copenhagen: A Smart City is a Better City. (2017). Erişim: 09 Nisan 2018, https://www.datamakespossible.com/copenhagen-smart-city-better-city/

D'Agostino, O. (2018). Smart City, modello di sviluppo sostenibile nell'interscambio dell'Unical con Santo Domingo. Erişim: 21 Haziran 2018, http://www.italiachiamaitalia.it/smart-city-modello-di-sviluppo-sostenibile-nellinterscambio-dellunical-con-santo-domingo/

Dameri, R. P. (2017). Smart City Implementation, 23–44. https://doi.org/10.1007/978-3-319-45766-6

Deloitte & Vodafone. (2016). *Akıllı Şehir Yol Haritası*, 12. Erişim: 30 Nisan 2018, https://www.sehirsizin.com/Documents/Deloitte-Vodafone-Akilli-Sehir-Yol-Haritasi.pdf

EasyPark. (2017). Erişim: 09 Nisan 2018, https://easyparkgroup.com/smart-cities-index/

Economic Policy Institute, Erişim: 11 Nisan 2018 http://www.epi.org/publication/manufacturing-job-loss-trade-not-productivity-is-the-culprit

Egan, P. (2017). GDPR: PREPARE NOW TO AVOID HARSH FINES FOR NON-COMPLIANCE. Erişim: 21 Haziran 2018, https://www.infogix.com/blog/gdpr-prepare-now-avoid-harsh-fines-non-compliance/

Evreka. (2018). Evreka Nedir? Erişim: 21 Haziran 2018, http://evreka.co/tr/nedir/

Facts about doing business in Copenhagen. (n.d.). *Business in Copenhagen - we can help free of charge*, Erişim: 5 Nisan 2018, http://www.copcap.com/invest-in-greater-copenhagen/faq

Flandorfer, P. (2012). Population Ageing and Socially Assistive Robots for Elderly Persons: The Importance of Sociodemographic Factors for User Acceptance. *International Journal of Population Research*, *2012*, 1–13. https://doi.org/10.1155/2012/829835

Gartner. (2017). Leading the IoT, Gartner Insights on How to Lead in a Connected World. *Gartner Research*, 1–29.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13–20. https://doi.org/10.1007/s11416-006-0015-z

Government of the Netherlands. (2016). Forms of cybercrime. Erişim: 18 Nisan 2018, https://www.government.nl/topics/cybercrime/forms-of-cybercrime

Harrison, C., Eckman, B., Hamilton, R., Hartswick, P., Kalagnanam, J., Paraszczak, J., & Williams, P. (2010). Foundations for Smarter Cities. IBM Journal of Research and Development, 54(4).

Hashem, I. A., Chang, V., Anuar, N. B., Adewole, K., Yaqoob, I., Gani, A., Ahmed, E., Chiroma, H. (2016). The role of big data in smart city. *International Journal of Information Management*, 748-758. doi:https://doi.org/10.1016/j.ijinfomgt.2016.05.002

Hongsong, C., Zhongchuan, F., & Dongyan, Z. (2011). Security and trust research in M2M system. *Proceedings of 2011 IEEE International Conference on Vehicular Electronics and Safety*. doi:10.1109/icves.2011.5983830

İETT İşletmeleri Genel Müdürlüğü. (2018). Mobiett Apple Store Mobil Uygulama Sayfası. Erişim: 16 Mayıs 2018, https://itunes.apple.com/tr/app/mobiett/id680243755

Istanbul Büyükşehir Belediye Başkanlığı. (2018). IBB Cep Trafik Apple Store Mobil Uygulama Sayfası. Erişim: 16 Mayıs 2018, https://itunes.apple.com/tr/app/ ibb-ceptrafik/id487589397

Istanbul Büyükşehir Belediye Başkanlığı. (2018). iTaksi Apple Store Mobil Uygulama Sayfası. Erişim: 16 Mayıs 2018, https://itunes.apple.com/tr/app/itaksi/id1301927766

Jackson, T. (2015). Can Africa fight cybercrime and preserve human rights?, Erişim: 17 Nisan 2018, from http://www.bbc.com/news/business-32079748

Jamalpur, S. (2017). I think using Machine learning in cyber security Enhances security to the next level. Erişim: 21 Haziran 2018, https://medium.com/@sainadhjamalpur/machine-learning-in-cyber-security-22f49b3ad2e3

K. Su, J. Li, and H. Fu. (2011). "Smart city and the applications," in Electronics, Communications and Control (ICECC), 2011 International Conference on. IEEE, pp. 1028–1031.

Kişisel Verileri Koruma Kurumu. (2016). Kişisel Verilerin Korunması Kanunu ve Uygulaması.

Kreyon. (2016). IoT Applications for Smart Cities, Erişim: 16 Mayıs 2018, http://www.kreyonsystems.com/Blog/iot-applications-for-smart-cities/

Kumar, V & Dahiya, B. (2017). *Smart Economy in Smart Cities*. https://doi.org/10.1007/978-981-10-1610-3

Lindskog, H. (2004). Smart communities initiatives. *Proceedings of the 3rd ISOneWorld Conference, (April)* 16.

Mohammed, F., Idries, A., Mohamed, N., Al-Jaroodi, J., & Jawhar, I. (2014). UAVs for smart cities: Opportunities and challenges. *2014 International Conference on Unmanned Aircraft Systems, ICUAS 2014 - Conference Proceedings*, 267–273. https://doi.org/10.1109/ICUAS.2014.6842265

Mohite, S., Kulkarni, G., & Sutar, R. (2013). *International Journal of Engineering Research & Technology (IJERT), 2*(9).

Moonshinenews. (2016). Cybersecurity operations center shield for new attacksç Erişim: 21 Haziran 2018, http://moonshinenews.com/cybersecurity-operations-center-shield-new-attacks/

Most Liveable City: Copenhagen Reclaims the Title Again. (n.d.) *Most liveable city copenhagen -The official website of Denmark*. Erişim: 5 Nisan 2018, http://denmark.dk/en/green-living/copenhagen/most-liveable-city-copenhagen.

Muscat, I. (2017). Cyber Threats vs Vulnerabilities vs Risks. Erişim: 16 Nisan 2018, https://www.acunetix.com/blog/articles/cyber-threats-vulnerabilities-risks/

Nam, T., & Pardo, T. A. (2011). Conceptualizing smart city with dimensions of technology, people, and institutions. In Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times (pp. 282–291). ACM.

Navarro, F. (2017). Urgent Microsoft security updates you need to get now! Erişim: 21 Haziran 2018, https://www.komando.com/happening-now/400232/urgent-microsoft-security-updates-you-need-to-get-now

Neirotti P, De Marco A, Cagliano AC, Mangano G, Scorrano F. (2014), Current trends in Smart City initiatives: Some stylised facts. 2014; 38:25–36.

Nie, X., & Zhong, X. (2013). Security In the Internet of Things Based on RFID: Issues and Current Countermeasures. *Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE 2013)*. doi:10.2991/iccsee.2013.297

Nuaimi, E. Al, Neyadi, H. Al, Mohamed, N., & Al-jaroodi, J. (2015). Applications of big data to smart cities. *Journal of Internet Services and Applications*. https://doi.org/10.1186/s13174-015-0041-5

O'Driscoll, A. (2018). *100+ Terrifying Cybercrime and Cybersecurity Statistics & Trends [2018 EDITION]*. Erişim: 17 Mayıs 2018, https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/

Oltsik, J. (2018, January 25). Artificial intelligence and cybersecurity: The real deal. Erişim: 21 Nisan 2018, https://www.csoonline.com/article/3250850/security/artificial-intelligence-and-cybersecurity-the-real-deal.html

Open Knowledge Foundation. (2012). Erişim: 8 Nisan 2018, www.opendatahandbook.org/guide/en/

Partridge, H. (2004). Developing a human perspective to the digital divide in the smart city. In Proceedings of the Biennial Conference of Australian Library and information Association (Queensland, Australia, Sep 21-24)

Polonetsky, J., & Wolf, C. (2009). How privacy (or lack of it) could sabotage the grid. *Smart Grid News*.

Pyzyk, K. (2018). Cities are 3-D printing their way to more sustainable futures. Erişim: 11 Nisan 2018, https://www.smartcitiesdive.com/news/3-d-printing-cities-sustainable-futures/520605/

Rahman, M. A., & Mohsenian-Rad, H. (2013). False data injection attacks against nonlinear state estimation in smart power grids. *2013 IEEE Power & Energy Society General Meeting*. doi:10.1109/pesmg.2013.6672638

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *Journal of Digital Forensics Journal of Digital Forensics, Security and Law*, *12*(2). Erişim: 8 Nisan 2018, https://commons.erau.edu/jdfsl/vol12/iss2/8

Schniederjans, D. G. (2017). Adoption of 3D-printing technologies in manufacturing: A survey analysis. *International Journal of Production Economics*, *183* (October 2016), 287–298. https://doi.org/10.1016/j.ijpe.2016.11.008

Scott, R. (2015). Manufacturing job loss: trade, not productivity, is the culprit

Simmhan, Y., Kumbhare, A. G., Cao, B., & Prasanna, V. (2011). An Analysis of Security and Privacy Issues in Smart Grid Software Architectures on Clouds. *2011 IEEE 4th International Conference on Cloud Computing*. doi:10.1109/cloud.2011.107

Solanas, A., Patsakis, C., Vlachos, I., Conti, M., Ramos, V., Falcone, F., . . . Perrera, D. N. (2014). Smart health: A context-aware health paradigm within smart cities. *IEEE Communications Magazine*, *52*(8), 74-81.

Starr, M. (2015). World's first 3D-printed apartment building constructed in China, CNET, p. 2016 Erişim:11 Nisan 2018, http://www.cnet.com/news/worlds-first-3d-printed-apartment-building-constructed-in-china

Symantec. (2010). Transformational smart cities: Cyber security and resilience.

Taşçı, U., Can, A. (2015). Türkiye'de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014. *Fırat Üniversitesi Sosyal Bilimler Dergisi*, Cilt: 25, Sayı 2, 229–248

Teknik ve Çevresel İdare Dairesi. (2015). Kopenhag Akıllı Şehir 2015, Şehir Bilgisi Raporu.

The Big Bang: How the Big Data Explosion Is Changing the World. (2013). Microsoft UK Enterprise Insights Blog - Site Home - MSDN Blogs. Erişim: 5 Nisan 2018, http://blogs.msdn.com/b/microsoftenterpriseinsight/archive/2013/04/15/ big-bang-how-the-big-data-explosion-is-changing-theworld.aspx

The Guardian. (2016). Team of hackers take remote control of Tesla Model S from 12 miles away. Erişim: 21 Haziran 2018, https://www.theguardian.com/technology/2016/sep/20/tesla-model-s-chinese-hack-remote-control-brakes

The Ministry of Housing, Urban and Rural Affair. (2015). Smart City Methods: From Ideas to Action, Case Examples. Erişim: 9 Nisan 2018, https://erhvervsstyrelsen.dk/sites/default/files/smart_city_2015_english.pdf.

The White House. (2009). National Cybersecurity Awareness Month, 2009

Torras, C. (2016). Service Robots for Citizens of the Future. *European Review, 24*(1), 17–30. https://doi.org/10.1017/S1062798715000393

UBC. (2017). October is Cyber Security Awareness Month. Erişim: 21 Haziran 2018, https://it.ubc.ca/news/october-cyber-security-awareness-month

United Nations. (2016). The World's Cities in 2016: Data Booklet. *Economic and Social Affair*, 29. https://doi.org/10.18356/8519891f-en

Wan, J., Li, D., Zou, C., & Zhou, K. (2012). M2M Communications for Smart City: An Event-Based Architecture. 2012 IEEE 12th International Conference on Computer and Information Technology. doi:10.1109/cit.2012.188

Washburn, D., Sindhu, U., Dines, R. A., Balaouras, S., Hayes, N. M., & Nelson, L. E. (2010). Helping CIOs Understand "Smart City" Initiatives: Defining the Smart City, Its Drivers, and the Role of the CIO.