

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 sağlamış 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 yapılacaktır 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 Saldırıları