AKILLI ŞEHİR BİLGİ GÜVENLİĞİ

Yrd. Doç. Dr. Hüseyin BAYRAKTAR [1], Dursun Yıldırım BAYAR [2], Ömer Faruk ERİŞ [3], Selami SUNGUN [4]

[1] Coğrafi Bilgi Sistemleri Genel Müdürlüğü, 06530, Çankaya, Ankara, huseyin.bayraktar@csb.gov.tr
[2] Coğrafi Bilgi Sistemleri Genel Müdürlüğü, 06530, Çankaya, Ankara, dyildirim.bayar@csb.gov.tr
[3] Coğrafi Bilgi Sistemleri Genel Müdürlüğü, 06530, Çankaya, Ankara, omerfaruk.eris@csb.gov.tr
[4] Coğrafi Bilgi Sistemleri Genel Müdürlüğü, 06530, Çankaya, Ankara, selami.sungun@csb.gov.tr

ÖZET

Ülkemizde akıllı şehir politikalarına ulusal katmanda bütüncül bir bakış açısı getirerek ulusal politikalarla uyumlu şekilde yatırımları güvence altına almak amacıyla 2020-2023 Ulusal Akıllı Şehirler Strateji ve Eylem Planı hazırlanmıştır. 2020-2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı kapsamında tanımlanan eylemlerin, görev ve sorumlulukların gerçekleştirilmesine ulusal ölçekte katkı sağlanması ve başta yerel yönetimlerimiz olmak üzere tüm paydaşların kapasitesinin artırılması amacıyla "Akıllı Şehirler Kapasite Geliştirme ve Rehberlik Projesi" T.C. Çevre, Şehircilik ve İklim Değişikliği Bakanlığı Coğrafi Bilgi Sistemleri Genel Müdürlüğü tarafından hayata geçirilmiştir. Proje kapsamında hazırlanan akıllı şehir külliyatında akıllı şehirlerde "bilgi güvenliği" konusu kapsamlı bir şekilde ele alınmış, bu konuda bilgi güvenliği eğitim kitabı, video ve sunumlar hazırlanmıştır.

Anahtar Sözcükler: akıllı şehirler, bilgi güvenliği, stratejik yönetim

ABSTRACT

SMART CITY INFORMATION SECURITY

The 2020-2023 National Smart Cities Strategy and Action Plan has been prepared in order to assure investments in line with national policies by bringing a holistic perspective to smart city policies at the national level in our country. Smart Cities Capacity Building and Guidance Project was implemented by the General Directorate of Geographic Information Systems of the Ministry of Environment, Urbanization and Climate Change, in order to contribute to the realization of the actions, duties and responsibilities that are defined within the scope of the 2020-2023 National Smart Cities Strategy and Action Plan, and to increase the capacity of all stakeholders, especially local governments. In the smart city collection prepared within the scope of the project, the issue of information security was comprehensively discussed, and a training book on information security, videos and presentations were prepared on this subject.

Keywords: smart cities, information security, strategical management

1. GİRİŞ

Akıllı şehir politikalarına ulusal katmanda bütüncül bir bakış getirerek birlikte çalışabilme yetisi kazanmak, belirlenen politikalarla uyumlu yatırımları önceliklendirerek yatırımların doğru proje ve faaliyetlerle uygulandığını güvence altına almak amacıyla ulusal ihtiyaçları ve öncelikleri bütüncül olarak göz önünde bulunduran, ekosistem paydaşlarının ortak aklı ile inşa edilen 2020-2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı hazırlanmıştır.

Günümüz dünyasında yönetim kavramı sadece işletmelerle sınırlanmamakta, teknolojiden sağlığa, savunma sistemlerinden bankacılığa birbirlerinden çok farklı alanlarda kullanılmaktadır. Bu kapsamda modern yönetim süreçleri; gelişen bilişim teknolojisini etkin kullanan disiplinler arası bir yapı olarak gelişimini sürdürmektedir.

Siber uzayın etkin kullanımı sonucunda çok büyük veri yığınları içerisinden kullanılabilecek veriler doğru ve hızlı olarak tespit edilebilmekte, belirlenen bu verilerle büyük bir doğrulukla analiz/sentez yapılabilmekte ve oluşturulan bu yeni verilerin çok hızlı bir şekilde paylaşılması sağlanabilmektedir.

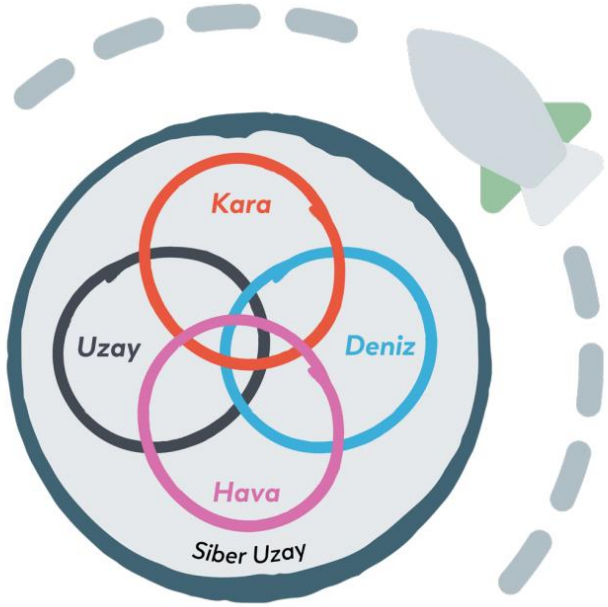
Siber uzayda gerçekleştirilen tüm süreçler, birbirlerinden farklı pek çok disiplinle etkileşim içindedir ve üretilen tüm ürünler sayısal kodlarla anılmaktadır. Bu sebeple üretilen tüm ürünlerdeki bu kodlar yani veriler, farklı değerler içermektedir. Bu değer ataması sayesinde de veri artık bir varlık olarak adlandırılmaktadır.

1.1 Siber Uzay

Bir varlık olarak adlandırılan verinin siber uzayın temel parçası olduğunu göz önüne aldığımızda, siber uzayın; insanlığın kara, deniz, hava ve uzay ortamlarında faaliyet gösterdiği dört boyuta ilave beşinci bir boyut olduğu da ortaya çıkmaktadır. ABD Silahlı Kuvvetleri "Siber Uzay Operasyonları Konsept Kabiliyet Planı 2016-2028" gibi güvenlik kaynaklarında siber uzay; "hava, kara, deniz ve uzaydan oluşan dört boyuta ilave beşinci boyut olarak adlandırılmaktadır. Bu boyutların her biri birbirlerinden bağımsız olmasına rağmen, bağlantı noktalarındaki her bir

boyutla siber uzayın irtibatlı olduğu" da ayrıca belirtilmektedir (fas.org). Bu durum Şekil 1'de temsili olarak gösterilmiştir.

Siber uzay her ne kadar sanal bir ortam olsa da bu ortamda yapılan faaliyetlerin fiziksel etkileri olmaktadır. Günümüz dünyasında en büyük güç olarak da değerlendirilen bilginin korunması büyük önem arz etmektedir. Bu bölümde bilgiyi korumak adına yapılan çalışmalar genelde bilgi güvenliği, özelde ise siber güvenlik anlamında incelenmektedir. Çünkü günümüz dünyasında "siber güvenlik" olgusunun hem kavramsal hem de etki olarak bilgi güvenliği kavramını kapsadığı değerlendirilmektedir.



Şekil 1. Güvenlik Boyutları

1.2 Bilgi Güvenliği ve Siber Güvenlik

Akıllı şehirleşmeyle kurumlar tarafından verilen hizmetlerde verimlilik, çevreyle etkileşimli olacak şekilde sürdürülebilir büyüme, şehirde bulunan insanların bireysel ya da toplu olarak ulaşımlarının kolaylaştırılması, kamu güvenliğine ek olarak doğal afetlere karşı şehir paydaşlarına güvenli/emniyetli ortam sağlama, şehrin ürettiği ekonomiyi iyileştirme ve bunun gibi alanları kapsamaktadır.

Şehirlerin küresel olarak birbirine bağlı olduğu bir ekonomide rekabet etme ve şehir sakinlerinin refahını sürdürülebilir bir şekilde sağlayabilme ihtiyacı ülkeleri ve şehirleri yeni teknoloji ve yenilikçi yaklaşımları değerlendirmeye yönlendirmektedir. Bu motivasyon, söz konusu teknoloji ve yaklaşımların getirdiği karmaşıklık ve değişim hızı ile geleneksel silo çözümleri geliştiren ekosistem paydaşlarını zorlamakta; şehir çözümlerinin bütüncül ve sistematik olarak ele alınması ihtiyacını ortaya çıkarmaktadır. Bu ihtiyacın karşılanmasında, paydaşlar arası iş birliği ile geliştirilen birlikte çalışabilir sistemlerin veri ve uzmanlığa dayalı olarak gelecek öngörüleriyle beklenti ve problemleri karşıladığını güvence altına alan Akıllı Şehir yaklaşımı çözüm olmaktadır.

Bu durumsal dönüşüm T.C. Çevre, Şehircilik ve İklim Değişikliği Bakanlığı 2020-2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı'nda detaylı olarak anlatılmaktadır. Bu kapsamda akıllı şehir ile amaçlanan:

- Şehrin mevcut ve gelecek beklenti ve problemlerini şehrin tüm mekânlarında ve sistemlerinde tetikleyici güç hâline getirmek,
- Fiziksel, sosyal ve dijital planlamayı birlikte ele alabilmek,
- Ortaya çıkan zorlukları sistematik, çevik ve sürdürülebilir bir şekilde öngörmek, tanımlamak ve karşılamak,
- Şehir içindeki organizasyonel yapılar arası etkileşimi sağlayarak bütünleşik hizmet sunumu ve yenilik üretme potansiyelini ortaya çıkarmaktır.

Akıllı Şehir, şehirlerin geleceği için statik bir yaklaşım tarif etmemektedir. Teknoloji ve verinin yenilikçi kullanımını organizasyonel değişimle birlikte gelecekteki şehirler için daha etkin, etkili ve sürdürülebilir yollarla farklı dinamik şehir vizyonlarının sunulmasına yardımcı olabilecek yönlendirici hususları ele almaktadır. Bir başka deyişle şehirlerin geleneksel olarak kullandıkları yönetişimi dönüştürmek hedeflenmektedir. Bir şehrin geleneksel yönetişim modeli, genellikle kullanıcı ihtiyaçları etrafında inşa edilmeyen, birlikte işlemeyen dikey silolar olarak çalışan işlevsel

yönelimli hizmet sağlayıcılarına dayanmaktadır. Akıllı Şehirlerin, bu dikey silolar arasında yenilik ve iş birliğini teşvik eden yeni işletim modelleri geliştirme ihtiyacı bulunmaktadır. Bu ihtiyacın karşılanmasında disiplinler arası yaklaşımlar yer almaktadır. Bu yaklaşımlardan biri de T.C. Çevre, Şehircilik ve İklim Değişikliği Bakanlığı 2020-2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı'nda da belirtildiği gibi akıllı altyapılar oluşturmaktır. Akıllı Altyapı kavramı; Akıllı Çevre, Akıllı Ulaşım ve İletişim Teknolojileri bileşenleri kapsamında kullanılan sensörlerle toplanan veriyi ileten, analiz eden, ölçen, izleyen ve daha gelişmiş performans ve kullanıcı deneyimi için kullanıcı taleplerine ve çevredeki değişikliklere akıllı şekilde yanıt verebilen ve kamusal değer oluşturan sistemler olarak tanımlanmaktadır.

Özellikle siber uzay göz önüne alındığında; siber teknolojilerin insanların hayat standartlarını artırdığı, çeşitli uygulamalarla insanın günlük yaşantısını kolaylaştırdığı ve bununla birlikte bireylerin, toplumun, kuruluşların ve hatta devletlerin güvenlik sınırlarını da bir oranda zorlayabildiği görülmektedir. İşte bu güvenlik hedefleri Şekil 2'de gösterildiği gibi erişilebilirlik, bütünlük ve gizlilik olmak üzere üç temel yapıda incelenebilir (ITU-T Rec., 2008). Bu üç unsur aynı zamanda bilgi güvenliği bileşenleri olarak da adlandırılmaktadır.

Erişilebilirlik: Bilgi ve bilgi sistemlerinin yetkisiz bozulmalara karşı korunmasıdır. Bilgi ve bilgi sistemlerine zamanında ve güvenilir bir şekilde erişilmesidir (Security 101, 2018).

Bütünlük: Bilgilerin yetkisiz düzenlenmesinin veya silinmesinin önlenmesidir. Bilgi ve bilgi sistemlerinin doğru, tam ve bozulmamış olmasının sağlanmasıdır (Security 101, 2018).

Gizlilik: Bilginin yetkisiz erişime veya açıklanmaya karşı korunması anlamına gelir. Bilgiye erişme hakkına sahip olanların bunu yapabilmelerini sağlarken, yetkilendirilmemiş kişilerin bunu yapmalarının engellenmesidir (Security 101, 2018).

Bilgi dediğimiz kavramın verilerin işlenmesi sonucunda elde edildiğini daha önce belirtmiştik. Kurumsal ya da bireysel olarak baktığımızda ürettiğimiz bilgileri ürettiğimiz ya da depoladığımız kaynakları,fiziksel ortamlar, elektronik ortamlar, insan ve bulunulan ortamlar olarak dört alt başlıkta incelemek mümkündür. Burada fiziksel ortamlar olarak; kâğıt, klasör, iş ya da özel mektuplar, faks çıktıları, çıktısı alınmış teknik raporlardan bahsedebiliriz. Elektronik ortamlar ise veri tabanları, bilgisayarlarda ya da harici belleklerde bulunan çeşitli dosyalar, e-postalar, sosyal medya verileri olarak özetlenebilir. Bunların içinde belki de en önemli bilgi kaynağı insanın kendisidir. Sayılan tüm bu bileşenler bir mekân içerisinde faaliyet gösterdiği için bulunulan ortamlar da önem arz etmektedir. İşte sayılan bu unsurların tamamının güvenliğini sağlamak ise kısaca "Bilgi Güvenliği" olarak adlandırılmaktadır.

Bilgi güvenliği ihlallerinde hedef alınan, tüm unsurların erişilebilirliği, bütünlüğü ve gizliliğine yöneliktir. Bu tehdit unsurları Şekil 3 incelendiğinde sadece kurumsal yapının içine yönelik bir yapılanma gibi algılanabilir. Ancak hemen tüm yapılarda siber uzay imkanlarından yararlanıldığı düşünüldüğünde tek başına bilgi güvenliği yeterli olmayacak, siber güvenlik boyutu da devreye girecektir. Siber güvenlik "siber çevre, organizasyonlar ve kullanıcının varlıklarını korumak için kullanılabilir araçlar, politikalar, güvenlik konseptleri, güvenlik önlemleri, kurallar, risk yönetimi, eylemler, eğitimler, uygulamalar ile teknolojiler bütünü" şeklinde tanımlanmaktadır (ITU-International Telecommunication Union, 2008).

1.3 Siber Güvenlik Yaşam Döngüsü

Siber uzayda geliştirilecek önlemlerin neredeyse tüm bilim dallarını içeren disiplinler arası bir yaklaşım olduğu göz ardı edilmemelidir. Siber teknik ve teknolojiler mühendisler tarafından geliştirilse de bu ürünlerin son kullanıcılarını her yaş grubundan insanlar oluşturmaktadır. Aynı zamanda siber uzayda gerçekleştirilen her tür faaliyet bir süreci tetiklemekte ve bu süreçler başka süreçlerle bütünleşerek adeta bir kartopu gibi büyüyerek yollarına devam etmektedir.

Tanımlama: Siber güvenlik riskini yönetmek için insanların, sistemlerin, varlıkların, verilerin ve yeteneklerin kurumsal bir anlayış içinde geliştirilmesini kapsar.

Koruma: Kritik hizmetlerin sunulmasınının sağlanması için potansiyel bir siber güvenlik olayının etkisinin sınırlandırılmasını veya gerekli önlemlerin geliştirilerek uygulanmasını içerir. Bu durumu gerçekleştirebilmek için dijital ve fiziksel varlıklara erişim kontrol edilmeli, verilerin güvence altına alınması için süreçler oluşturulmalı ve koruyucu teknolojiler kullanmalıdır.

Algılama/Tanıma: Siber güvenlik ihlallerinin hızlı bir şekilde tanımlanması faaliyetlerini belirtir. Algılama işlemi, siber güvenlik olaylarını oluşturan anomalilerin zamanında fark edilmesini kapsar.

Cevap Verme: Tespit edilen bir siber güvenlik olayıyla ilgili önlem almak için uygun faaliyetleri geliştirmeyi ve uygulamayı ifade eder. Bunun için bir cevap planı hazırlanmalı, dost iletişim hatları tanımlanmalı, etkinlikler hakkında bilgi toplanmalı ve analiz edilmeli, kötücül olayı ortadan kaldırmak için gerekli tüm aktiviteler gerçekleştirilmelidir.

Kurtarma: Siber güvenlik olayı nedeniyle bozulmuş olan tüm yetenekleri veya hizmetleri geri yüklemek için uygun aktiviteler geliştirmeyi ve uygulamayı kapsar.

2. SONUÇLAR

Günümüz dünyasında en büyük güç olarak değerlendirilen bilginin korunması büyük önem arz etmektedir. Akıllı şehrin en önemli varlıklarından olan ve sürdürülebilirliğinin sigortası olan bilgi güvenliğine yönelik olarak; akıllı şehir kapsamında gerçekleştirilen faaliyetlere ve sahip olunan varlıklara ilişkin kritik altyapıların bilgi güvenliği politikalarının ve yönetişiminin tanımlandığı bir mekanizmaya ve bunu gerçekleştirecek organizasyon yapısının ulusal ve yerel katmanda oluşturulmasına ihtiyaç duyulmaktadır.

Günümüz siber saldırılarının –çoğunlukla- yapay zekâ yazılımları yardımıyla gerçekleştirilmesi, bu sızma faaliyetlerinin hedef bilgi sistemleri tarafından zamanında saptanamamasına sebep olabilmektedir. Bu kapsamda hedef bilgi sistemi korumasında da yapay zekâ yöntemleri kullanımına öncelik verilerek "tehdit belirleme hızı"nın artırılması yönünde projeler geliştirilmesi üzerinde durulmalıdır.

Kritik altyapı donanım ve yazılımları başta olmak üzere, hassas teknoloji için gerekli tüm yazılımların milli kaynak kodları içermesi ve mevcut yazılım oluşturma standartlarına uygun bir şekilde yazılması sağlanmalıdır.

Tüm kurum ve bireylerin siber güvenlik stratejilerini ve siber güvenlik uygulama politikalarını güncel tutmaları, üretilen politika ve stratejiler kapsamında kısa, orta ve uzun vadeli siber güvenlik uygulama planlarını oluşturmaları büyük önem kazanmaktadır.

Bu planlamaların toplumdaki siber uzaya erişim sağlayan tüm yaş grupları ve bilgi seviyelerine göre sosyal katmanları kapsamalıdır. Bu katmanlarda; siber güvenlik farkındalığı ile siber güvenlik bilinci oluşturacak ve katmanlar arasında da etkileşimi sağlayacak şekilde değişik seviyelerde siber güvenlik eğitimleri tasarlanmalıdır. Bu eğitimler uygulamalı bir şekilde gerçekleştirilmelidir.

KAYNAKLAR

ABD Silahlı Kuvvetleri; "Siber Uzay Operasyonları Konsept Kabiliyet Planı 2016- 2028" http://www.fas.org/irp/doddir/army/pam525-7-8.pdf [17.01.2018]

Holsapple, C.W. (2008). Decisions and Knowledge, (Ed.) Handbooks on Decision Support Systems 1:Basic Themes. Berlin: Springer.

IAEA Nuclear Security Series No. 17, p. 38. Austria https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf [14.11.2019].

ITU-International Telecommunication Union. (2008). https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Introduction%20 to%20the%20Concept%20of%20IT%20Security.pdf pg.43 (Erişim Tarihi 19.02.2018).

ITU-T Rec. X.1205 (2008) "Overview of cybersecurity", https://www.itu.int/ rec/T-REC-X.1205-200804-I, (Erişim Tarihi 22.01.2018).

Resmi Gazete (2013). Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, http://www.udhb.gov.tr/doc/siberg/SOME_2013-2014_EylemPlani.pdf (Erişim Tarihi 19.02.2018).

Security 101, https://www.cmu.edu/iso/aware/presentation/security101-v2. pdf, (Erişim Tarihi 22.01.2018).

T.C. Çevre Şehircilik ve İklim Değişikliği Bakanlığı, 2021. bilgi güvenliği/ https://www.akillisehirler.gov.tr/egitim-bilgi-guvenligi, (Eylül 2022).

T.C. Çevre, Şehircilik ve İklim Değişikliği Bakanlığı (2019). 2020-2023 Akıllı Şehirler Stratejisi ve Eylem Planı.