39. BÖLÜM / CHAPTER 39

SAĞLIK ALANINDA SİBER GÜVENLİK VE YAPAY ZEKANIN ROLÜ

THE ROLE OF CYBER SECURITY AND ARTIFICIAL INTELLIGENCE IN HEALTHCARE

Yalçın ÖZKAN*, Çiğdem SELÇUKCAN EROL**,***

*Dr., Emekli Öğretim Üyesi, İstanbul, Türkiye

E-mail: yalcin2006@gmail.com

Doç.Dr., İstanbul Üniversitesi Enformatik Bölümü, *Fen Fakültesi Biyoloji Bölümü Botanik ABD,
İstanbul, Türkiye

E-mail: cigdems@istanbul.edu.tr

DOI: 10.26650/B/ET07.2021.003.39

ÖZ

Sağlık alanı bilgi teknolojilerinin (BT) kullanıldığı en önemli alanlardan biridir. Hastane bilgi sistemlerinde ve tıbbi cihazlarda yıllardır kullanılan bu teknoloji, nesnelerin internetinin (IoT: *Internet of Things*) yaygın kullanımıyla beraber, hastaların bedenlerinde taşıdığı akıllı tıbbi cihazlarla daha da yaygınlaşmaktadır. Başlangıçta veriyi depolamak, ihtiyacımız olduğunda ulaşmak, analiz etmek, raporlamak gibi amaçlar için kullandığımız BT, günümüzde tüm cihazları birbirleriyle konuşturmak hatta öğrenen makineler (yapay zeka) geliştirmek gibi hedeflerle ilerlemektedir. Diyabet hastasının bedenine bağlı bir insülin pompası, hekimin mobil cihazları ile konuşarak insülin salınımını dengeleyebilmektedir. Cihazların birbirleriyle ve bizlerle “iletişim” halinde olduğu bu ağ, her yenilikte olabileceği gibi, hayatımızı kolaylaştırmasının yanı sıra beraberinde daha önce bilmediğimiz risk ve tehditleri de getirmektedir. Bu risk ve tehditler her alanda elbetteki önemlidir ama sağlık alanında insan hayatını doğrudan ya da dolaylı olarak etkilemesi nedeniyle BT’ nin kullanıldığı diğer alanlardan da biraz daha fazla dikkat ve önem gerektirmektedir. Siber suçlular, sağlık alanında kullanılan siber ortamlarda en masum olarak hastaların verisine göz dikmektedir. Akıllı tıbbi cihazların kullanılması siber suçluların gözünü hastaların sağlığına hatta canlarına çevirmektedir. Bu çalışmada sağlık alanında siber güvenliğin önemine ve yapay zekanın bu alanda kullanımına dikkat çekmek amaçlanmaktadır. Bu amaçla siber güvenliğin tanımından sonra siber saldırı örneklerine yer verilerek bilgi edinilmesine katkı sağlanmaya çalışılmıştır. Sağlık alanında veri güvenliği örnek olaylarla irdelenerek konunun önemine yönelik farkındalık artırılmaya çalışılmıştır. Yapay zekanın kendisine ilişkin güvenlik riskleri bu araştırmanın kapsamına dahil edilmemiştir. Sonuç olarak, sağlık alanında bilgi teknolojilerinin kullanımı konusunda daha fazla bilgi edinmek, çaba sarf etmek, zaman ayırmak ve maddi olarak yatırım yapmak gerektiği düşünülmektedir. Önleyici tedbirler yapay zeka ile desteklenebilir ancak insan odaklı olarak çalışmalar mutlaka yürütülmelidir. Bilinçlendirme, farkındalık oluşturma, sözleşme ve hatta politikalarla zorunluluklar oluşturulmalıdır.

Anahtar Kelimeler: Sağlık alanında siber güvenlik, sağlık alanında siber riskler, siber güvenlikte yapay zeka,

medjacking

ABSTRACT

Health care is one of the most important areas where information technologies (IT) are employed. This technology, which has been used in hospital information systems and medical devices for years, is becoming more widespread with the smart medical devices that patients carry on their bodies with the rapid growth of the Internet of Things (IoT). IT, which we use to store data in the beginning and to access, analyze, and report when we need it, nowadays has progressed with the goals of making all devices talk to each other and even developing learning machines (artificial intelligence). An insulin pump connected to the body of a patient with diabetes can balance insulin secretion by talking to the physician's mobile devices. This network, in which the devices "communicate" with each other and with us, maybe in every innovation, as well as making our lives easier. It also brings along risks and threats that we did not know before. These risks and threats are of course important in every field, but they require a little more attention and importance in the field of health, as they affect human life directly or indirectly than other areas where IT is used. Cyber criminals overlook patients' data as the most innocent in cyber environments used in health care. The use of smart medical devices turns cyber criminals' eyes on patients' health and even their lives. This study aims to draw attention to the importance of cybersecurity in the field of health and the use of artificial intelligence in this field. For this purpose, after the definition of cybersecurity, it has been tried to contribute to obtaining information by including examples of cyberattacks. In the field of health, data security was examined with case studies, and awareness of the importance of the issue was tried to be increased. This study does not include the security risks of artificial intelligence. As a result, it is believed to be necessary to learn more about the use of information technologies in the field of health, to try, to spend time, and to invest financially. Preventive measures can be supported by artificial intelligence, but human-oriented studies must also be conducted. Obligations should be created through awareness raising, contracts, and even policies.

1. Siber güvenlik ve veri güvenliği

Siber güvenlik, siber ortamda kuruluşların ve kullanıcıların sahip olduğu varlıkları korumak için kullanılabilecekleri araçlar, politikalar, güvenlik kavramları, güvenlik önlemleri, yönergeler, risk yönetimi yaklaşımları, eylemler, eğitim, en iyi uygulamalar, güvence ve teknolojilerin toplamı olarak kabul edilir. Siber güvenlik, siber ortamdaki ilgili güvenlik risklerine karşı kuruluşun ve kullanıcının varlıklarının güvenlik özelliklerine ulaşılmasını ve sürdürülmesini sağlamaya çalışır (Solms ve Niekerk, 2013).

Veri güvenliği, en kritik iş varlıklarınızı, bir başka deyişle verileri yetkisiz veya istenmeyen kullanımlara karşı koruma sürecidir. Veri güvenliği, kuruluşların gelirlerini korumasını, dijital dönüşümü kolaylaştırmasını, yasal düzenlemelere uymasını ve müşteri sadakati oluşturmalarını sağlar. Veri güvenliği günümüzün dijital işletmeleri için kritik bir farklılaştırıcı olarak da değerlendirilebilir. Veri hemen hemen her organizasyonun kalbinde yer alır ve iş değerini artırmak için etkili kullanımı kolaylaştırırken aynı zamanda onu korumak da önemli bir başarı faktörüdür (IBM, 2020).

Bazı verilere erişime, bu bilgileri koruma altına almak amacıyla sınırlamalar getirilmesi mümkündür. Kişisel veri, bu açıdan bakıldığında erişiminin denetim altına alınması gereken

başlıca veri kaynakları olarak düşünülebilir. Bunun dışında sağlık verisi, kurumsal veri, ülke güvenliği ile ilgili veri bu tür önemli bilgi kaynakları arasında sayılabilir. Veri güvenliği bu bilgiyi kullanan, depolayan ve ileten sistemler ile donanım dahil, kritik unsurlar olarak tanımlanmaktadır (Whitman ve Mattord, 2009).

2. Siber tehditler

Siber güvenlik tehdidi veya bir başka deyişle siber tehdit, kişilerin yada kurumsal yapıların sahip olduğu veriye zarar vermeye çalışan kötü amaçlı eylemlerdir. Bu tür zararlı eylemler arasında verinin çalınması, dijital yaşamı bozmaya kalkışılması, bunun da ötesinde ekonomik ve sosyal sonuçlar yaratarak mevcut sistemleri tahrip etmeye çalışan faaliyetler sayılabilir. Sözü ettiğimiz bozucu ve yıkıcı etkiler yaratılması için siber saldırılar düzenlenir. Bu saldırılar arasında bilgisayar virüsleri, veri ihlalleri, hizmet reddi (*DoS; Denial of Service*) atakları sayılabilir. Siber saldırılar siber uzay denilen ve kullanılan dijital cihazlardan oluşan bir sanal ortamdan yapılmaktadır. Bizlere hizmet vermeyi amaçlayan bu cihazların oluşturduğu uzayın, artık bize zarar vermeyi amaçlayan dijital silahları da barındırmaya başlaması, yeni düşmanları anlamamıza yardımcı olan bir metafor haline geldi (Taylor, 2020).

Tıbbi verinin küresel olarak sayısallaştırılması ve özellikle IoT'lerin yaygınlaşması sağlık sektörü tedavi yetenekleri ve operasyonel etkinlikleri için oldukça önemli bir başarı olsa da, saldırganlara daha fazla olasılık yarattığı da bir gerçektir. Günümüzde siber veri ihlali, sağlık sektörü için önlem almayan tıbbi kurumların en ciddi finansal risklerinden biri haline gelmiştir. Sağlık kurumları siber saldırının neden olduğu veri ihlali ile ilgili finansal riski düzgün bir şekilde yönetebilmek için böyle bir durumda ortaya çıkabilecek potansiyel maliyetlerin farkında olmalıdır (Meisner, 2017).

3. Sağlıkta veri güvenliği

Sağlıkta veri güvenliği denildiğinde, hangi tür verinin koruma altında olması gerektiği konusu önem kazanmaktadır. *HIPAA (The Health Insurance Portability and Accountability Act)* tarafından bu konuda bazı tanımlamalar ve kurallar yayınlanmıştır. Genel olarak aşağıda belirtilen konularda veri güvenliği söz konusu olmaktadır (Beckers, 2015);

- a) İsimler,
- b) Doğum tarihleri, ölüm tarihleri, tedavi tarihleri, kabul tarihleri ve taburcu tarihleri,
- c) Telefon numaraları, faks numaraları ve diğer iletişim bilgileri,
- d) Adresler,

- e) Sosyal Güvenlik numaraları,
- f) Tıbbi kayıt numaraları,
- g) Fotoğraflar ve karşılaştırılabilir görüntüler,
- h) Parmak, retina ve sesli kayıtlar dahil biyometrik tanımlayıcılar,
- i) Diğer tanımlayıcı numaralar.

Özellikle sağlık verisinde veri güvenliğinin sağlanması açısından gelişmiş ülkeler başta olmak üzere, çoğu ülkede yasal düzenlemelerin yapılması yoluna gidilmektedir. Örneğin ABD'deki *HIPAA* yasası bu açıdan önemli özelliklere sahiptir. *HIPAA* yasası, öncelikle sağlık veri akışını modernleştirmek, sağlık ve sağlık sigortası endüstrileri tarafından tutulan kişisel olarak tanımlanabilir bilgilerin sahtekarlık ve hırsızlığa karşı nasıl korunması gerektiğini ve sağlık sigortası kapsamındaki sınırlamaları ele almak için oluşturulmuştur (*HIPAA*, 2020).

Avrupa Birliği'nin kabul ettiği veri gizliliği düzenlemeleri dünyanın en katı veri güvenliği yasaları arasındadır. Bu yasalar Avrupa Birliği'nin tüm üyelerinde geçerlidir. Bu yasaya göre kişisel veriler ve hassas olarak değerlendirilen kategorideki veriler ancak bazı koşullar altında toplanabilir. Toplanan verilerin yanlış kullanımından korunması ve kişisel verilerin sorumluluğu veriyi toplayan mekanizmalara yüklenmiştir. Avrupa Birliği sağlık politikaları sağlıkta hasta verisinin gizliliği ve güvenliği konusunda bazı temel ilkelere odaklanılması konusudur. Bu temel ilkeler şu şekilde özetlenebilir (Archer 2019):

- a) Kişilerin kişisel sağlık verisinin ve bu konudaki haklarının korunması,
- b) Veri toplama ve işlenmesinde şeffaflığa uyulması,
- c) Kişisel veri ihlallerinin bildirilmesi zorunluluğu,
- d) Verilere erişim, güncelleme, silme veya engelleme haklarının düzenlenmesi,
- e) Veri ihlallerinde ciddi cezai yaptırımların uygulanması.

ABD ve Avrupa Birliği'nin sağlık verisinde veri güvenliği konusunda ciddi yaklaşımları olmasına rağmen, yasal mevzuat yaklaşımında bazı farklılıklar söz konusudur. Avrupa Birliği'nin tüm ülkelerinde veri güvenliği mevzuatı aynı şekilde uygulanmasına karşılık, ABD'de tam bir standart uygulamadan söz edemeyiz. ABD'de sağlık verilerinin korunmasında her eyaletin farklı uygulamaları bulunmaktadır (Archer 2020).

4. Veri ihlali

Veri ihlali, hassas olarak değerlendirilen, korunan veya gizli olduğu ilan edilen verinin, yetkisiz bir kişi tarafından kopyalandığı, iletildiği, görüntülendiği, çalındığı veya kullanıldığı bir güvenlik ihlalidir. Kurumsal yapılarda müşteri verisinin bir personel tarafından sözlü, sözsüz veya yazılı olarak dağıtılması bile veri ihlali olarak değerlendirilebilir (Wikipedia, 2020).

ABD’de kurulu *HHS (Health and Human Services Office for Civil Rights)* dairesi tarafından veri ihlalleri, bilgisayar korsanlığı/BT olayları, yetkisiz erişim/ifşa, verinin çalınması, veri kaybı ve yanlış veri imhası olmak üzere beş türe ayrılarak izlenmektedir (HHS, 2020). ABD’de 2019 yılındaki sağlık veri ihlalleri incelendiğinde, bilgisayar korsanlığı/BT olayları sınıflı veri ihlallerinin çoğunlukla gerçekleştiği görülmektedir (Tablo 1).

Tablo 1. ABD 2019 yılı sağlık veri ihlallerinin dağılımı (HIPAA, 2019)		
İhlal	Olayların sayısı	İhlal Edilen Kayıt Sayısı
Bilgisayar Korsanlığı / BT Olayları	303	36.210.097
Yetkisiz Erişim / Ifşa	147	4.657.932
Çalınma	39	367.508
Kayıp	15	74.271
Yanlış imha	6	26.081

4.1 . Veri ihlallerinin maliyeti

Günümüzde veri ihlallerinin korkutucu bir hal aldığı ve yarattığı etkinin önemli boyutlara ulaştığı bilinmektedir. Özellikle finansal kurumların bu saldırılara hedef olması dikkat çekicidir. Bilgisayar saldırganlarının, kişisel ve hassas bilgileri (Ör: kredi kartı, banka, sosyal güvenlik bilgileri) elde etmeye uğraştıkları görülmektedir. Bu saldırılar sonucunda veri ihlalleri doğal olarak kişisel ve kurumsal yapıların önemli kayıplar yaşamasına neden olmaktadır. Ponemon Institute tarafından yürütülen ve IBM Security tarafından desteklenen 2019 yılı veri ihlali maliyeti raporu, dünyadaki veri ihlallerini ve bu ihlallerin maliyetlerini ortaya koymaktadır (IBM Security, 2020).

2019 yılı veri ihlalleri sektörel bazda incelendiğinde, bu ihlallerin neden olduğu ortalama toplam maliyetleri karşılaştırma olanağı elde edilir. Şekil 1’de yapılan sektörel karşılaştırmaya göre, organizasyon bazında 6.45 milyon dolar ortalama maliyet rakamıyla sağlık sektörünün en başta yer aldığı anlaşılır. Veri ihlallerinin zirvesinde olan sağlık sektörünü finans, enerji, endüstri ve ilaç sektörleri izlemektedir.

Şekil 1. Sektörlere göre milyon dolar cinsinden veri ihlallerinin yarattığı ortalama toplam maliyetler (IBM Security, 2020)

Veri ihlallerinin maliyeti ülkeler veya bölgeler itibariyle analiz edildiğinde, Şekil 2’de görüldüğü gibi, ABD en başta gelmektedir. ABD’nin 2019 yılı veri ihlalleri maliyetinin organizasyon başına 8.19 milyon dolar olarak gerçekleştiği tahmin ediliyor. Bunu 5.97 milyon dolarla Orta Doğu bölgesi, 4.78 milyon dolarla Almanya, 4.44 milyon dolarla Kanada ve 4.33 milyon dolarla Fransa izlemektedir. Tüm dünya ülkeleri göz önüne alındığında organizasyon bazında ortalama maliyet 3.92 milyon dolar, Türkiye’de ise bu maliyet 1.86 milyon dolar olarak tahmin edilmiştir.

Şekil 2. Ülkelere veya bölgelere göre milyon dolar cinsinden veri ihlallerinin yarattığı maliyetler (IBM Security, 2020)

Veri ihlallerinin en önemli göstergelerinden birisi de bu saldırılardan etkilenen kişi sayısıdır. ABD’de 2019 yılında ortaya çıkan veri ihlalleri göz önüne alındığında ilk beş veri ihlali Tablo 2’de belirtildiği biçimdedir. Veri ihlallerinin etkilediği kişi sayısı açısından ABD’de Optum360 şirketinin 11.5 milyon müşterisinin bu saldırıdan etkilendiği anlaşılmaktadır.

Tablo 2. ABD 2019 yılı en büyük sağlık veri ihlalleri ve etkilenen bireyler (HIPAA, 2019)		
Veri ihlaline uğrayan kurum	Etkilenen Birey sayısı	İhlalin Türü
Optum360, LLC	11.500.000	Bilgisayar Korsanlığı / BT Olayı
Laboratory Corporation of America Holdings dba LabCorp	10.251.784	Bilgisayar Korsanlığı / BT Olayı
Dominion Dental Services, Inc., Dominion National Insurance Company, Dominion Dental Services USA, Inc.	2.964.778	Bilgisayar Korsanlığı / BT Olayı
Clinical Pathology Laboratories, Inc.	1.733.836	Yetkisiz Erişim / İfşa
Inmediata Health Group, Corp.	1.565.338	Yetkisiz Erişim / İfşa

Tablo 2’de yer alan veri ihlalleriyle ilgili birinci sırada yer alan vakayı biraz daha derinlemesine inceleyecek olursak, birbirleriyle ilişkili şirketlerde ortaya çıkabilecek bir zafiyetten söz edilebilir. ABD’deki tahlil laboratuvarlarının en önemlilerinden biri olan Quest Diagnostics, 2019 yılında yaklaşık 11-12 milyon civarında hasta verisinin kopyalanarak çalındığını bildirdi. Bu olay 2019 yılının sağlık sektöründeki en büyük veri ihlali olarak kayıtlara girdi. Bir fatura tahsilatları servis sağlayıcısı olan *American Medical Collection Agency (AMCA)*, bu hizmeti yerine getirebilmek için *Quest Diagnostics* dahil olmak üzere çeşitli müşterilerinden alınan kişisel bilgilerini yüklemektedir. Ancak 2019 yılında *AMCA* sistemlerinde yer alan *Quest Diagnostics* firmasının yüklenicisi olan *Optimum360* şirketine ait kişisel verilerle saldırganın erişebildiği ve kopyaladığı anlaşılmıştır. Bilgisayar korsanları isim, kişisel bilgi, sosyal güvenlik numaraları, finansal bilgiler ve tıbbi bilgiler gibi bilgileri içeren sistemlere erişimi elde etmişlerdir. Buna karşılık saldırganların laboratuvar test sonuçlarına erişemedikleri düşünülmektedir. Siber güvenlik uzmanlarına göre, çevrimiçi ödemeler, özellikle kişisel ve sağlık bilgileri finansal kaygılarla birlikte ortaya çıkabiliyorsa, bu şekildeki karmaşık yapılar güvenlik riskleri taşıyabilir. Riskler, kimlik bilgisi doldurma, XXS gibi istemci tarafı güvenlik açıklarının yanı sıra uzaktan kod yürütme ve sunucu tarafı istek sahteciliği dahil, sunucu tarafı güvenlik açıklarını içerebilir. Ödeme, QuestDiagnostics örneğinde olduğu gibi bir alt yüklenicinin var olduğu durumlarda, her iki tarafın da API’lerin güvenliği söz konusu olduğunda daha fazla endişe edilmesi gerekir. Bilindiği gibi, internet işlemlerinin sadece insanlar ve onları koruyan araçlar kadar güvenli olduğu unutulmamalıdır (Pennic, 2019).

5. Tıbbi cihazlara yönelik siber saldırılar – *medjacking*

Hastalara doğrudan zarar vermeye veya hastaları tehdit ederek bir menfaat elde etmeye yönelik *çökertme* (hacking) işlemine girişmeye *medjacking* adı verilmektedir (Breene, 2016). Siber güvenlik ile ilgili alanda kullanılmaya başlanan bu kavram, sağlık alanında çok önemli bir tehlikeye işaret etmektedir.

Medjacking, özellikle hastane ağlarında arka kapılar oluşturarak tıbbi cihazların ele geçirilmesini amaç edinmektedir. Bunu önlemede hastanelerin bilişim teknolojileri, bu cihazların konumlandırılmasında söz sahibi olamadıklarından, denetimi sağlamada ve bölümleri siber saldırganlar için arka kapıları önlemede zorluklarla karşılaşmaktadırlar. Bir hastanede yatak başına on veya onbeş cihazın ağa bağlı olması normal bir durum olarak değerlendirilir. Durum böyle olunca, saldırganların sistemlere sızması ve hasta verilerine erişim açısından çok uygun bir ortam yaratıldığı anlaşılmaktadır (Rai, 2016).

Eski teknolojilere dayalı medikal sistemlere saldırganların erişimi nispeten daha kolaydır. Yaşam destek ve teşhis araçlarının bir kısmı eski ve standart işletim sistemlerini kullanır. Bu durum saldırganların uygun dijital saldırı araçlarını edinerek savunmasız tıbbi cihazlara erişimde işini daha da kolaylaştırır (DiGiacomo, 2017). Farklı türde ve sayıca fazla tıbbi cihazların bulunduğu bir sağlık kurumunda saldırganların sadece bir cihazı ele geçirmeleri bile tüm sistemi tehdit altına sokabilir ve saldırgan ağdaki daha değerli veriye sahip diğer tüm kaynaklara da erişim olanağı elde edebilir.

İlk medjack saldırısı ile 2015 yılında karşılaşıldı. Bu saldırıda saldırganlar arka planda kullanılan ve saldırılara karşı güvenliği olmayan tıbbi cihazlara erişmeyi başardılar. Bu saldırılar gelişigüzel yapıldı ve belirli bir hedefleri bulunmuyordu. 2016 yılındaki saldırılarda ise saldırganlar daha gelişmiş araçlarla saldırılara başladılar. Bu kez ağlara sızmak için arka kapıları ve botnet'leri kullanmaya başladılar. Özellikle eski windows işletim sistemine sahip cihazlara karşı etkili oldular. 2017 yılından itibaren saldırganların daha karmaşık yöntemler kullanmaya başladıkları fark edildi. Artık *MRI* (*magnetic resonance imaging*) ve *CT* (*computerized tomography*) tarayıcılarının da hedef haline gelmeye başlamıştır. Windows XP, Windows Server 2003 gibi işletim sistemine sahip cihazların diğerlerine göre nispeten savunmasız olduğu anlaşıldı. Gerekli güvenlik yamalarına sahip olmayan işletim sistemlerinin tıbbi cihazlara karşı yapılan saldırıların daha başarılı olmasına yol açtığı anlaşıldı. En önemlisi, tıbbi cihazlara yapılan saldırıların daha hedeflenerek yapılmaya başlandığı gözlemlendi (Sheridan, 2017).

Tıbbi cihazlarda ortaya çıkabilecek açıkları kapatmak ve güvenliği sağlamak üzere kullanılan yazılımlar için “yama” adı verilen ek bakımlara gereksinim duyulur. Bu tür yazılım yamaları bir tür “aşı” olarak da görülebilir. Klinisyenlerin, kullanıcıların bu tür cihazların güvenliğine zarar vermeden, düzenli olarak “aşılmalı” talep edebilecekleri tahmin ediliyor (Tully ve ark. 2018).

Hastalıkların izlenmesi ve tedavisi için bağlı cihazlar daha yaygın ve güçlü hale gelmektedir. Bu yaygın kullanım alanı daha da genişledikçe medjacking olasılığının arttığı bir noktaya

doğru hızla yaklaşıldığı görülmektedir. İletişim teknolojilerinin gelişmesi ile birlikte sağlık izleme ve görüntüleme faaliyetleri de etkilenmeye başlamıştır. Özellikle sağlıkla ilgili giyilebilir ve implante edilebilir sensörlerin, monitörlerin ve kablosuz uzaktan iletişim yeteneklerine sahip cihazların yükselişi görüldü (Armstrong ve ark. 2015).

Cihazların çeşitlenmeye başlamasıyla birlikte, bu cihazların hem kendi güvenlikleri, hem de diğer bilişim sistemleri için ve doğal olarak veri kaynakları için bir risk oluşturmaya başladığı ve siber saldırganların ilgisini çekmeye başladığı görülmektedir. Günümüzde aktif bir tıbbi cihazın tanımlanan işlevleri yerine getirebilmesi için bir bilgisayar ortamı ile ağ ortamında iletişim halinde olması gerekir. Bilgisayar korsanının bir tıbbi cihazın kontrolünü ele geçirebilmek için ağdaki bilgisayarı ele geçirmesi yeterlidir (Ayala, 2016).

5.1. İnsülin pompası saldırısı

Tıbbi cihazlara yapılan saldırılar sağlık kuruluşlarını endişeye sevk etmektedir. Örneğin bazı insülin pompalarında güvenlik zafiyetleri ile karşılaşmıştır. Mevcut riskler, Medtronic'in MiniMed insülin pompaları ile kan şekeri ölçüm cihazları, sürekli glukoz izleme sistemleri, uzaktan kumanda ve bu pompalarla birlikte kullanılan CareLink USB cihazı gibi diğer cihazlar arasındaki kablosuz iletişim ile ilgilidir. FDA tarafından uyarılan firma, cihazda belirlenen siber güvenlik açıkları nedeniyle, hasta, bakıcı veya sağlık uzmanı dışında bir kişinin potansiyel olarak yakındaki bir MiniMed insülin pompasına kablosuz olarak bağlanıp pompanın ayarlarını değiştirebileceği tespit edilmiştir. Bunun anlamı, gerekli önlemleri almayan bu cihazları her an bir saldırgan cihaz ayarlarını istediği gibi değiştirerek hastaya aşırı insülin iletilmesine, hipoglisemiye (kan şekeri düşüklüğü) yol açmasına veya insülin iletimini durdurmasına, yüksek kan şekeri ve diyabetik ketoasidoza (kanda keton asit birikmesi) yol açabilir. Bu güvenlik açıkları karşısında firmanın söz konusu cihazlarının tümünü sağlık kurumlarından geri çekmiştir (FDA, 2019).

İnsülin pompalarına yönelik bir diğer siber saldırı örneği Johnson&Johnsons tarafından 2008 yılında piyasaya sürülen bir üründe rastlandı. Belirlenen güvenlik açıklarının bu cihazları uzaktan erişim ile saldırıları gerçekleştirebilecekleri anlaşıldı. Saldırganın sisteme erişimi ile birlikte, pompa cihazı ile uzaktan kumanda ünitesi arasındaki bağlantının kesilebileceği, saldırganın kendi komutlarını girmeye başlayabileceği, hastanın düzenli insülin dozunu artırabileceği ve böylece aşırı doz sınırının aşılabileceği; böylece hipoglisemik reaksiyonların oluşumuna yol açılabileceği belirlendi. Saldırgan, telsiz ekipmanı kullanırken saldırıyı gerçekleştirmek için 90 metrelik bir mesafede olabilir. Eğer ekipman daha güçlü ise, saldırgan 1 ila 2 km mesafeden bir saldırı başlatabilir. Söz konusu insülin pompalarındaki güvenlik açıklarını

herhangi bir saldırı olmadan siber güvenlik uzmanları ortaya çıkardığı için bu sayede gerçek anlamda bir saldırının önü alınmıştır (HackRead, 2016).

Johnson&Johnsons yöneticileri Reuters’e verdiği bilgide, söz konusu insülin pompası olan cihaza erişmeye çalışan bir saldırganla karşılaşmadıklarını iletiler. Şirket yine de müşterilerini uyararak sorunun nasıl çözüleceği konusunda önerilerde bulundu (Finkle, 2016).

5.2. Görüntü cihazlarına saldırı

Eski görüntüleme cihazları ve eski tıbbi bilişim sistemleri güvenli ve güncel olmayan işletim sistemlerine sahip olmaları nedeniyle siber saldırganlar açısından kolay hedeflerdir. Genellikle bu fonksiyonlar, beklenen ömürlerinin ötesinde yıllar boyunca korunur, bu sistemler siber saldırılar için “pivot noktaları” görevi görür. Bilgisayar korsanlarının tıbbi bilgi teknolojisi sistemlerine girebileceği zayıf bağlantılardır. Pek çok sağlık kurumunda ise görüntü birimleri ile hastanenin genel bilgi sistemi entegre olduğundan, görüntü birimlerinin yarattığı bu zafiyetinden yararlanarak hastanenin hayatı veri kaynaklarına erişim olanağı elde edilebilmektedir. Eski işletim sistemlerine sahip bilgisayar sistemlerinde görüntü cihazlarına musallat olan ilk saldırı *Conficker* isimli bilgisayar solucanı idi. Microsoft Windows’un ilk sürümlerindeki zayıflıklardan yararlanan *Conficker*, ilk olarak 2008’de tespit edildi. 2009’un başında kaybolmasına rağmen, hizmetlerde kullanılan eski sistemler nedeniyle, sağlık sistemlerinde yeniden görülebilmektedir. Bu tür bir saldırı görüntü cihazlarını savunmasız hale getirmektedir. Bir hastanenin onkoloji servisinde rastlanan bu saldırının amacı, röntgen cihazlarının yarattığı bu açık kapıdan girerek hastanenin bilgi ağına sızmak idi. Bilgisayar korsanı bu amacına ulaşmıştır (Freiherr, 2017).

5.3. Kardiyak cihazlara yönelik saldırılar

Kalbin daha düzenli çalışmasına yardımcı olmak üzere tasarlanan ve işlevleri birbirine benzeyen iki cihazdan söz edilebilir. Bunlardan birincisi kalp pili, diğer ise defibrilatör adı verilen cihazlardır. Her iki cihaz için siber güvenlik açıklarının önemli olduğu ve hayati sonuçlara neden olabileceği üzerine güvenlik kuruluşlarının, sağlık kurumlarının ve bu cihazları üreten firmaların endişeleri olduğu bilinmektedir.

5.3.1. Kalp pillerine yönelik saldırı

Siber saldırıların sağlıkta tehlike yarattığı alanlardan birisi de kalp pilleriyle ilişkilidir. İlk kalp pili saldırısı yaklaşık oniki yıl önce gerçekleştirildi. Bu saldırı ve daha sonrakiler pek karmaşık değildi ve kalp piliyle ilgili basit biçimde radyo komutlarını değiştirmeye yönelikti. Ancak son zamanlarda daha karmaşık ve büyük tehdit oluşturan saldırılarla karşılaşmaktadır.

Bu saldırılar doğrudan implante edilmiş kalp pilleri üzerine kötü amaçlı yazılımların bulaştırılması sonucunda gerçekleşir. Örneğin, Medtronic altyapısında kalp pillerini uzaktan kontrol etmek için kullanabilecekleri güvenlik açıkları keşfedildi (Newman, 2018).

Günümüzde kalp pillerinin çalışma esası, üzerine yerleştirilen bir mikroçipe dayanmaktadır. Bu işlemci kalp pilinin çeşitli algılama ve eylem görevlerini kontrol etmede devreye girmektedir. Söz konusu bu mikroişlemci, kalp pilinde tüm süreçlerin yapıldığı, kalbe gönderilecek şokun ayarlanmasını sağlar, kalpten ölçümler alır, hastalara ve tıbbi bakım sağlayıcılarına destek vermeye çalışır. Kalp pillerinin yönetimi, ürettiği verilerin alınması benzeri işlemler için hasta veya bakım personeli tarafından kontrol edilebilen bir bilgisayara uzaktan bağlı olması söz konusudur. Bu tür bir bilgisayar sistemindeki basit seviyedeki güvenlik zafiyetleri bile siber saldırganların ilgisini çekebilir. Kablosuz erişim yapılabilen bu bilgisayara erişimi elde eden saldırganlar artık kalp pilini de ele geçirmiş durumdadır ve hastaya gönderilebilecek güçlü bir şok, kalp pilinin tamamen düzgün çalışmasını önleyerek hayati sorunlara neden olabilir. Bir kalp pilini kullanan kişiye zarar vermek amacıyla saldırı düzenlenebildiği gibi, güvenlik açısından “arka kapı” olarak değerlendirilebilecek bu sistemi, sağlık kurumunun sahip olduğu diğer verilere, örneğin tıbbi hasta kayıtlarına erişim için bir geçit olarak da kullanabilir. Hatta arka kapı yoluyla ele geçirilen kalp pillerine de zararlı yazılımlar yüklenebilmektedir (Boulos ve ark., 2016).

Kalp piliyle suikaste uğranması olayı Homeland gibi bazı dizilerin de konusunu oluşturdu. 2007’de dönemin ABD Başkan yardımcısı Dick Cheney, güvenlik kaygısıyla kendi kalp pilinin kablosuz bağlantı işlevini devre dışı bıraktırdığını açıklamasına ve günümüzde yarattığı zafiyetlere rağmen kalp pillerinin kablosuz iletişim özelliğinin hastaları evde takip etmek açısından çok yararlı olduğu düşünülmektedir (Vallance, 2015).

5.3.2. Defibrilatör saldırıları

Kalbin elektriksel sinyallerini görüntüleme, durmuş veya durmakta olan kalbe belli bir süre ve belli bir miktarda elektrik akımı vererek, kalbi normal kardiyak ritmine kavuşturmak amacıyla defibrilatörler kullanılabilir. Bu cihazlar normal kalıcı kalp pillerine benzer. Ancak nlar ilave olarak hayati risk oluşturabilen ritim bozukluklarının tedavisinde kullanılabilen bazı özel yeteneklere ve şok tedavisi verebilme özelliklerine sahip cihazlardır (Loukas, 2015).

Defibrilatörler, ciddi aritmi ve kardiyomiyopati gibi hayatı tehdit eden kalp rahatsızlıkları olan insanların hayatlarını kurtarmak için üretilen elektronik cihazlardır. Ancak şimdi, İç Güvenlik Bölümüne (DHS) göre, Medtronic defibrilatörler, bilgisayar korsanlarının cihazı “kısa menzilli erişim” içinde uzaktan kontrol etmesine izin veren siber saldırılara karşı savunmasızdır (FDA, 2019).

Bu uyarıya göre, potansiyel saldırganlar, Medtronic cihazlarından veri okuyan ve doktorlara aktaran monitörler arasındaki kablosuz iletişim sistemindeki güvenlik açıklarından yararlanabilirler. Saldırganlar, iletilen ve hassas verilere erişim sağlayan Medtronic ürünleri tarafından kullanılan ‘Conexus’ telemetrisi ile güvenlik protokollerini aşabilecekleri, böylece cihazların saldırıya açık olduğu anlaşıldı (Staines, 2019).

6. Tıbbi Cihazlardaki Güvenlik Açıkları için *FDA*’nın yaklaşımı

Cihazların güvenliği dışında genel anlamda siber güvenlikle açıklıkların belirlenmesi ve saldırıların önlenmesi konusunda önemli gelişmeler yaşanmaktadır. Ancak aynı kanaati tıbbi cihazlara yönelik olarak söyleyemiyoruz. Günümüze dek, tıbbi cihazların güvenliklerini ele alma ve çözümler üretme konusunda nispeten çok az bir ilerleme kaydedildi. Amerikan gıda ve ilaç dairesi olan *FDA* bu konuda bazı öneriler geliştirmeye ve güvenlik ile ilgili endişelerini dile getirmeye başlamış; ancak bu tür güvenlik sorunları olan cihazların satılmasına izin vermiştir. *FDA* cihazların güvenliği konusunda uyarı ve rehberlik hizmetlerini yerine getirmektedir (DiGiacomo, 2017).

Siber saldırılara hedef olan tıbbi cihazların yarattıkları tehditler göz önüne alındığında, ülkelerde özellikle merkezi sağlık organizasyonları bu konuya eğilme gereksinimi duymuşlardır. Bu konuda öncü organizasyonların başında U.S.Food & Drug Administration, yani *FDA*’nın geldiğini söyleyebiliriz. Tıbbi cihazların pazarlanması öncesinde, bu cihazların tasarımında ve geliştirilmesinde siber güvenlikle ilgili göz önünde bulundurulması gereken sorunlar *FDA* tarafından bir kılavuz çerçevesinde 2014 yılında yayınlanarak üreticilerin dikkati çekildi (FDA, 2014). Bu kılavuzun ardından, *FDA* tıbbi cihaz üreticileri için pazarlama sonrası süreç için bazı önerileri içeren bir siber güvenlik kılavuzunu bu kez 2016 yılında yayınladı (FDA, 2016). Bu kılavuz, tıbbi cihazların piyasaya sürüldükten sonra siber saldırılara karşı korunmada izlenecek yol ile ilgili önerileri kapsamakta, özellikle cihaz üreticilerinin kullanımında karşılaşılan güvenlik açıklarının rapor edilmesiyle ilgili izlenecek yolu ve raporlama çalışmalarını içermekte ve bu tür olaylarla ilgili olarak iletişim kanallarının geliştirilmesi gerektiği vurgulanmaktadır. *FDA* cihazlara yönelik saldırı tehditlerinin ve güvenlik açıklarının belirlenmesi açısından bazı önerilerde bulunmaktadır. Bu önerileri, a) Güvenlik açıklarının son kullanıcılar ve hastalar üzerindeki etkilerinin belirlenmesi, b) güvenlik açığından doğabilecek hasarların belirlenmesi, c) risk seviyesinin belirlenmesi, riski azaltma stratejilerinin göz önüne alınması ve d) risk kabul kriterlerinin belirlenmesi biçiminde özetleyebiliriz. Bu kılavuz tıbbi cihazların kullanılmaya başlanmasıyla birlikte siber saldırılara karşı daha iyi korumak ve prosedürler geliştirmek için yararlı bir kaynak olarak kabul edilmektedir.

7. Sağlık tesislerine yönelik siber riskler

HIMSS (Healthcare Information and Management Systems Society) sağlık ve sektörler arası siber güvenlik raporu (2019) sağlık alanında siber güvenlik ile ilgili ne gibi sorunlar olduğuna dair sektörler arası bir bakış açısı sunmaktadır. Bu raporda, güvenlik araçlarında ve yazılımlarında bulunan önemli güvenlik açıklarına da işaret ediliyor. Örneğin *SSL* sertifikaları için rastgele sayı oluşturmada bir zafiyet olduğu bu rapor ile açıklandı (HIMSS, 2019).

HIMSS araştırmasına göre, hastaneler üzerinde siber saldırıların ardındaki temel motivasyon tıbbi kimlik hırsızlığı, hırsızlık ve çalıntı hastane bilgilerinin satışı, karaborsa ve hatta hasta bilgilerine yetkisiz erişim ve hırsızlık vardır. Bununla birlikte, bir siber saldırının bir hastanedeki sonuçları, tıbbi bilgilerin çalınması veya ihlali ile sınırlı değildir, aynı zamanda bu kuruluşların klinik ve operasyonel uygulamaları ile ilişkili diğer riskleri de içerir. Hastanelerin altyapılarını ve elektronik korunan sağlık bilgilerini saldırılara karşı savunmak için ciddi, stratejik ve yapısal önlemler almaları gerekmektedir. Aksi taktirde teknolojilerin ve ekipmanların düşmesi veya kullanılamaması, kuruluşun operasyonel sürekliliğine ve sonuç olarak ciddi tehditlere neden olabilir (ehCOS, 2020).

Bilgisayar korsanlarının sağlık tesislerine ve hasta bilgilerine erişim konusunda çok istekli olmasının bazı nedenleri vardır. Her şeyden önce, hasta verileri kolayca satılabilmektedir ve bu da sağlık tesislerinin bu kadar çok saldırıya maruz kalmasının en önemli nedeni olarak görülmektedir. Karaborsada sağlık kayıtları ve hasta ile ilgili diğer bilgiler büyük ölçüde talep edilmektedir. Bazı durumlarda, bilgisayar korsanları bilgileri hastanenin kendisine geri satabilmektedir. Bilgisayar korsanları şantaj yoluyla veya bu tür kayıtları en yüksek teklif sahibine satarak hasta verilerinden para kazanabilmektedir. Bilgisayar korsanları, yüksek profilli hastaların bilgilerini de kullanabilir. Örneğin 2017’de saldırganlar Londra’daki büyük bir plastik cerrahi kliniğinin ağını ihlal ettiler. Bu bilgiler resimlerden, tıbbi kayıtlardan, adreslerden ve hatta hassas finansal verilerden oluşuyordu. Bilgisayar korsanlarının sağlık tesislerini hedef almalarının bir başka nedeni olarak, bu kurumların güçlü güvenlik önlemlerine sahip olmamaları ve güvenliğin sağlanması konusunda geri kaldıkları gösterilebilir (Silver, 2020).

7.1. Sağlık tesislerine yönelik Siber Saldırıları

Bazı tıbbi cihazlara yapılan siber saldırıları ele alarak inceledik. Bu güvenlik ihlalleri genellikle yerel ağlarda uzaktan erişim yoluyla gerçekleştirilir. Sadece tıbbi cihazlar değil, sağlık kurumlarının sunucu tabanlı bilgi teknolojileri de tehdit altındadır. Üstelik bu tür saldırıların amacı sadece cihazı kullanan kişi değil, hastalar dahil sağlık kurumunun tüm varlıklarıdır. Bu nedenle sunuculara yapılan üç saldırı biçimini; kaba kuvvet, hizmet reddi ve *XXS web* saldırılarını kısaca açıklayabiliriz.

7.1.1. Brute force - kaba kuvvet saldırıları

Kimlik doğrulama; şifresi bilinmeyen bir sisteme deneme-yanılma yoluyla şifre girişleri yapılarak zorla girmeye çalışmak mümkündür. Doğal olarak bu tür bir girişi yapanlar bir siber saldırgan olarak değerlendirilir ve yapılan eylem kaba kuvvet saldırısı olarak kabul edilir. Saldırgan doğru şifreyi buluncaya dek denemelerine devam eder. Ancak bu şekildeki rastgele denemelerle iyi şifrelenmiş sistemlere giriş mümkün değildir. Onun yerine saldırganlar alternatif yöntemler geliştirmiştir. Bunlar arasında kapsamlı anahtar arama işlemi sayılabilir. Saldırgan, doğru şifreyi bulana kadar olası tüm şifreleri ve parolaları sistematik olarak kontrol eder.

Alternatif olarak, saldırgan bir anahtar türetme fonksiyonu kullanarak şifreden anahtarı tahmin etmeye çalışabilir. Anahtar türetme fonksiyonu, gizli bir anahtar değerinden veya sahte bir rastlantı işlevi kullanarak parola veya parola gibi bilinen diğer bilgilerden bir veya daha fazla gizli anahtarı türetmekte kullanılır. Parola tahmininde, bu yöntem kısa şifreleri kontrol etmek için kullanıldığında çok hızlıdır, ancak daha uzun şifreler için kaba kuvvet saldırılarındaki aramalar çok uzun sürdüğü için “şifre sözlüğü” gibi diğer yöntemleri kullanılır (En.wikipedia, 2020).

Burada saldırgan, şifre olarak kullanılabilecek milyonlarca kelime içeren bir şifre sözlüğü kullanır. Saldırgan kimlik doğrulaması için bu şifreleri tek tek dener. Bu tür deneme işlemleri için otomatik şifre kırma işlemlerinde kullanılmak üzere hazırlanmış saldırı araçları da bulunmaktadır (Şekil 3).

Şekil 3. Siber güvenlikte kaba kuvvet saldırıları. (<https://www.manageengine.com/log-management/cyber-security-attacks/what-is-brute-force-attack.html>)

7.1.2. DDoS siber saldırıları

Günümüzün etkili ve sonuçları bakımından en tehlikeli görülen siber saldırısı, bir sunucuya ağ trafiğinin aşırı derecede yönlendirilmesi ve sunucuyu çalışmaz hale getirilmesidir. Hizmet reddi (DoS) adı verilen bu saldırı, saldırganın bir hedef sunucuya aşırı derecede meş-

gul ederek diğer kullanıcıların bu sunucuya erişimlerinin engellenmesi olarak tanımlanır. Eğer birden fazla kullanıcı trafiği bu hedefe yönlendirilirse bu kez dağıtılmış hizmet reddi (*DDoS; distributed denial of service*) saldırılarından söz edilir. Bu tür saldırılar çoğunlukla devlet kuruluşları, sağlık kurumları, bankalar ve bunun gibi önemli tesislerdir. Böyle olunca hedef tesislerde bir süre verilen hizmetlerin tamamen durmasına neden olunmakta, bunun sonucunda hasarlar ve kayıplar söz konusu olmaktadır.

DDoS saldırılarının yapılabilmesi için, saldırgan dışında çok sayıda başka sunuculara ve bilgisayar sistemlerine gereksinim duyulur. Bunu temin etmek için saldırgan saldırıya girmeden önce bir hazırlık dönemine girer. Bu dönemde başka sunucuların da kendi emrinde olmasını ister. Saldırgan diğer bilgisayarlara diğer sızma yöntemleriyle botnet adı verilen zararlı yazılımları yerleştirir ve beklemeye başlar. Hedef sunucu belirlendikten sonra bu hedefe emrinde olan tüm bilgisayar sistemlerini aynı zamanda yönlendirerek bir *web* trafiği yaratır (Şekil 4). Bu trafiğin boyutları, hedef sistemlerin kapasitesine göre çoğunlukla büyüktür ve hedef bilgisayar bu ağ trafiğiyle baş edemeyerek kilitlenir, böylece hizmet vermeyi tamamen durdurur. Hedef bir sağlık kuruluşu ise saldırının yaratabileceği etki çok daha büyük olabilir. Sağlık kuruluşlarındaki ana sunucuya bağlı tüm bilgisayar sistemleri ve bağlı tıbbi cihazlar devre dışı kalır. Saldırının şiddetine göre sağlık hizmetleri önemli oranda aksaklığa uğrayabilir. *DDoS* saldırıları belirli bir sağlık kuruluşunu hedef almayabilir. Saldırı sağlık kuruluşunun tedarikçilerini hedef alarak dolaylı yünden zarar vermeye çalışabilir (Ayala, 2016).

2014 yılında Boston Çocuk Hastanesi'nde böyle bir saldırı ile karşılaşıldı. Ebeveynler arasında yaşanan bir velayet tartışması, Boston Çocuk Hastanesi'ni bir saldırının hedefi haline getirdi. Tartışmaya *Anonymous* isimli saldırı grubunun bir hak ihlali olduğunu öne sürerek tepki göstermesine neden olmuştur. *Anonymous*, cezalandırmak amacıyla hastanenin ağına *DDoS* saldırıları düzenleyerek harekete geçti ve bunun sonucunda da Harvard Üniversitesi ve tüm hastaneleri de içeren bu ağdaki internet bağlantısı kilitlendi ve doğal olarak bu ağda verilen tüm hizmetler olumsuz yönde etkilendi (CIS, 2020).

Şekil 4. DDoS saldırıları (<https://www.f5.com/labs/articles/education/what-is-a-distributed-denial-of-service-attack->)

7.1.3. Web saldırıları-XSS

Siber saldırganların kullandıkları bir diğer yöntem siteler arası komut dosyası oluşturma/ çalıştırma (XSS; *cross site scripting*) saldırılarıdır. Bu saldırı, Şekil 5 üzerinde görüldüğü biçimde, kötü amaçlı komut dosyalarının başka türlü iyi huylu ve güvenilir *web* sitelerine enjekte edildiği bir tür enjeksiyon türüdür. XSS saldırıları, bir saldırgan, genellikle bir tarayıcı tarafı komut dosyası biçimindeki kötü amaçlı kodun, bir *web* uygulaması yardımıyla farklı bir son kullanıcıya gönderilmesi suretiyle gerçekleştirilir. Son kullanıcı tarayıcısının, komut dosyasına güvenilmemesi gerektiğini bilmesi mümkün değildir ve komut dosyasını çalıştırır. Komut dosyasının güvenilir bir kaynaktan geldiğini düşündüğü için, kötü amaçlı komut dosyası tarayıcı tarafından tutulan ve o siteyle kullanılan tüm çerezlere, oturum bilgilerine veya diğer hassas bilgilere erişebilir. Bu komut dosyaları *HTML* (*hyper text markup language*) sayfasının içeriğini bile yeniden yazabilir (Cloudflare, 2020).

Şekil 5. XSS web saldırıları (Cloudflare, 2020).

8. Sağlık siber güvenliğinde yapay zeka

Sağlık hizmetleri, siber risklerle diğer sektörlerden daha fazla karşı karşıya gelmektedir (Tosun vd., 2019). Sağlık alanında yapay zeka uygulamaları oldukça yaygın bir alana hizmet vermektedir. Üstelik yapay zekanın hastalıkların keşfi gibi temel sağlık hizmetlerinde insanlardan daha iyi hizmet verebileceği konusunda görüşler oluşmaya başlamıştır. Örneğin, günümüzde yapay zeka algoritmalarının, kötü huylu tümörleri tespit etmede, radyologlardan daha iyi performans gösterebileceği anlaşılmıştır (Davenport ve Kalakota 2019). Genetik ve kanser araştırmalarında yapay zeka ve makine öğrenmesi algoritmaları yoğun biçimde kullanılmaktadır. Yapay zeka alanında özellikle derin öğrenme algoritmaları, kanser araştırmalarında hastalık tanısı ve risk faktörlerinin belirlenmesinde kullanılabilmektedir. Bunun yanı sıra görüntü işleme ile sağlık alanında gelişkin tanı olanakları sunmaktadır (Özkan ve Erol, 2019).

Sağlık alanında siber saldırıların algılanmasında da yapay zeka algoritmaları geniş olanaklar sunmaktadır. Sağlık tesislerine yönelik siber riskler bölümünde ele aldığımız *DDoS* saldırılarının sağlık alanında çok ciddi sonuçlara neden olabileceğinden söz ettik. Bu tür saldırıların sağlık kurumunun özellikle ana sunucularını hizmet vermektan alıkoyan ve o sunuculardan verilen hizmetlerin tamamen durmasına neden olan ağ saldırılarıdır. Bir ağa yapılan *DDoS* saldırıları makine öğrenmesinin denetimli veya denetimsiz öğrenme algoritmaları yardımıyla belirlenebilir. Eğer denetimli öğrenme uygulanacaksa, ağ trafiği verilerinin öncelikle etiketlenmesi gerekir. Etiketli veri kümesi kullanılarak makine öğrenmesinin derin öğrenme algoritmaları yardımıyla öngörü modeli elde edilir ve bu model kullanılarak ağdaki her bir hareketin normal bir erişim olup olmadığı veya bir *DDoS* saldırısı olup olmadığını tahmin ederek

sunucuyu uyarır. Bu tür saldırılarda makine öğrenmesinin diğer geleneksel algoritmaları da kullanılabilmesine karşılık, derin öğrenme algoritmalarının daha iyi öngörü performansına sahip olduğunu söyleyebiliriz.

Yukarıda sözü edilen *DDoS* saldırılarının etiketlenerek denetimli öğrenme yöntemleriyle öngörülebilmesine karşılık, siber güvenlikte saldırının ne tür olduğu değil, herhangi bir saldırının olup olmadığını anlamak da önemli olmaktadır. Bu durumda sorun bir anomali algılama problemine dönüşür. Bu kez veri kümeleri önceden etiketlenmez ve makine öğrenmesinin denetimsiz öğrenme algoritmaları devreye girer. Bu algoritmalar içinde yer alan otomatik kodlayıcılar (*autoencoders*) adı verilen derin öğrenme yöntemine başvurulabilir. Bu yöntem etiketsiz veri kümelerini kullanarak kendi kendine öğrenmeyi gerçekleştirir. Böylece elde edilen model ağ trafiği verilerinde öngörü yapmak amacıyla kullanılır.

Web sayfalarına erişimdeki anomali durumlarını tespit etmek söz konusu olduğunda *web* trafiği zaman serilerine başvurulur. Derin öğrenmenin geri dönüşlü ağırları içinde yer alan *LSTM* (*long short-term memory*) algoritması bu tür tahmin işlemlerinde başarıyla kullanılabilir. Bu yöntem istatistiksel zaman serilerinde kullanılan *ARIMA* modelleri ile aynı amaca yönelik olmasına karşılık, doğrusal olmayan modeller yaratarak daha başarılı öngörülerde bulunabilir.

Yapay zeka algoritmalarının kullanılabileceği bir diğer alan botnet ve *XSS web* saldırılarıdır. Bu tür tehlikeli saldırıları belirlemek üzere makine öğrenmesinin denetimli öğrenme algoritmaları yanı sıra gerektiğinde denetimsiz veya kendi kendine öğrenen algoritmalarından yararlanılır. Sağlık kurumlarına yapılan bu saldırılar doğal olarak anonim adresler kullanılarak gerçekleştirilmeyebilir. Saldırganlar karanlık internetin *TOR* ağı yardımıyla izlerini kaybederek, sunucuların güvenlik duvarlarını rahatça aşabilirler. Bu durumda ağ trafiğinde *TOR* tarayıcısından yapılan erişimlerin algılanması söz konusu olduğunda yapay zekanın denetimli öğrenme algoritmaları devreye girebilir.

Yapay zekanın kendisine ilişkin güvenlik riskleri bu araştırmanın kapsamına dahil edilmemiştir. Bu konuda bilgi edinmek için, Çokar (2019), Ozan Özparlak (2019) ve Say (2018)'in çalışmaları önerilmektedir.

9. Sonuç

Siber güvenlik, *BT*'nin kullanıldığı ortamları ve dolayısıyla bu ortamların bağlı olduğu çevrelerini korumaktadır. Konu sağlık alanında *BT*'nin kullanıldığı ortam ise bu ortam, hastaya, sağlık çalışanlarına ya da hastaneye ait veriyi içermektedir. Bu noktada **veri güvenliği**

önplana çıkmaktadır. Günümüzde veri güvenliği ciddi güvenlik sorunlarından birisi olarak görülmektedir. Pek çok ülke veri ihlallerinin önüne geçebilmek için teknik tedbirlerin ötesinde veri güvenliği konusundaki yasal önlemleri geliştirmektedir. Veri ihlallerinin ortaya çıkardığı ekonomik kayıpların boyutları göz önüne alındığında siber saldırılara karşı kurumları dayanıklı hale getirmenin önemi ortaya çıkmaktadır. Kaygı duyulması gereken en önemli noktalardan birisi, siber saldırıların özellikle sağlık kurumlarını ve sağlık cihazlarını hedef almaya başladığının anlaşılmasıdır.

En fazla sağlık sektörünün siber saldırılarla karşı karşıya kaldığı gerçeği, bu sektörde siber güvenliğin hasta güvenliği kadar önemli bir konu olduğunu ortaya koymaktadır. Hastaların kullandığı ağ tabanlı sağlık cihazlarının bağlı olduğu bilgisayarlardaki siber güvenlik açıkları, hem bu tür cihazların kontrolünün korsanların eline geçmesine neden olmakta, hem de sağlık kurumunun diğer bilgisayar ve sunucuları için bir arka kapı oluşturmakta, böylece tüm sağlık hizmetlerini tehlikeye atabilmektedir. Bu açıdan bakıldığında, ağ üzerindeki veri trafiğinin yapay zeka algoritmaları ile denetlenmesi ve ona göre bir savunma stratejisi geliştirilmesi sağlanabilir.

Sağlık alanında, BT'nin kullanıldığı ortam, hastaların bedenlerine bağlı akıllı tıbbi cihazlar ise bu noktada veri güvenliğinden ziyade **can güvenliği** söz konusu olabilmektedir. Günümüzde tıbbi cihazlarda yapay zekanın kullanımının yaygınlaşmaya başladığı görülmektedir, ancak yapay zeka da bir siber ortam ürünüdür ve kendine özgü risk ve tehditler de içermektedir. Sonuç olarak sağlık alanında BT kullanımı için donanımdan daha fazla yazılıma odaklanılması, özellikle sürdürülebilirlik noktasında yazılımların güncellenmesi konusu dikkate alınmalı, network göz ardı edilmemeli, bu alana yönelik personel ve maddi destekler gerekirse arttırılmalıdır. Daha fazla bilgi edinme, bilinçlendirme çalışmalarının yanı sıra geçmiş deneyimlerden ve mevcut veriden yararlanarak önleyici tedbirlere başvurulmalıdır. Yapay zeka veriden öğrenme noktasında destekleyici bir unsur olarak kullanılabilir.

Kaynakça / References

- Archer, (2020), "The Importance of Healthcare Data Security", 02/02/2020 tarihinde erişildi, <https://archer-soft.com/en/blog/importance-healthcare-data-security>
- Armstrong DG, Kleidermacher DN, Klonoff DC, Slepian MJ (2015), "Cybersecurity regulation of wireless devices for performance and assurance in the age of medjacking.", J Diabetes Sci Technol., 10:435-438, <https://journals.sagepub.com/doi/10.1177/1932296815602100>
- Armstrong DG, Kleidermacher DN, Klonoff DC, Slepian MJ (2015), "Cybersecurity regulation of wireless devices for performance and assurance in the age of medjacking.", J Diabetes Sci Technol., 10:435-438, <https://journals.sagepub.com/doi/10.1177/1932296815602100>
- Ayala, L., (2016), "Cybersecurity for Hospitals and Healthcare Facilities: A Guide to Detection and Prevention", Apress, Berkeley, CA

- Baranchuk,A., Refaat,M.M., Patton,K.K., Chung,M.K., Krishnan,K., Kutyla,V., Upadhyay,G., Fisher,J.D., Lakkireddy,D.R., (2018), “Cybersecurity for Cardiac Implantable Electronic Devices-What Should You Know?”, Journal of the American College of Cardiology, vol. 71 no. 11 1284-1288.
- Beckers, (2015), “50 things to know about healthcare data security & privacy”, Whitepaper, 11/03/2020 tarihinde erişildi: <https://www.beckershospitalreview.com/healthcare-information-technology/50-things-to-know-about-healthcare-data-security-privacy.html>
- Boulos, P., Sargolzaei, A., Ziaei, A., Sargolzaei, S., (2016), “Pacemakers: a survey on development history, cyber-security threats and countermeasures”, Int. J. Innov. Stud. Sci. Eng. Technol, vol. 2, no. 8, 2016, <http://ijisnet.org/wp-content/uploads/2016/08/IJISSET-020808.pdf>
- Breene, K., (2016), “What is medjacking?”, World Economic Forum, 2/12/2020 tarihinde erişildi, <https://www.weforum.org/agenda/2016/10/medjacking-health-cyber-risk-explainer/>
- CIS, (2020), “DDoS Attacks: In the Healthcare Sector”, 18/03/2020 tarihinde erişildi:<https://www.cisecurity.org/blog/ddos-attacks-in-the-healthcare-sector/>
- Cloudflare, (2020), “What Is Cross-Site Scripting?”, 19/03/2020 tarihinde erişildi: <https://www.cloudflare.com/learning/security/threats/cross-site-scripting/>
- Çokar, M., (2019), “Sağlıkta Yapay Zeka, Kuramsal Çerçeve ve Etik”, Sağlık Bilimlerinde Yapay Zeka, Eds. Bulut, M., Dilmen, N., Esmer, G. B., Gezer, M., Selçukcan Erol, Ç., Türker Şener, L., Çağlayan yayınevi, ISBN 9789754361674, sf 211-230.
- Davenport, T., & Kalakota, R. (2019), “The potential for artificial intelligence in healthcare”, Future healthcare journal, 6(2), 94–98, DOI: <https://doi.org/10.7861/futurehosp.6-2-94>
- DiGiacomo, J., (2017), “Medjacking is a Real Threat to Health Care Systems“, 12/3/2020 tarihinde erişildi, <https://revisionlegal.com/internet-law/data-breach/medjacking/>
- ehCOS, (2020), “Cybersecurity in Hospitals: Prevention as a Defense From Attacks”, 21/03/2020 tarihinde erişildi: <https://www.ehcos.com/en/cybersecurity-in-hospitals-prevention-as-a-defense-from-attacks/>
- En.wikipedia, (2020), “Brute-force attack”, 25/03/2020 tarihinde erişildi: https://en.wikipedia.org/wiki/Brute-force_attack
- FDA, (2014), “Content of premarket submissions for management of cybersecurity in medical devices: guidance for industry and food and drug administration staff”, 23/Mart/2020 tarihinde erişildi, <https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf>
- FDA, (2016), “Postmarket management of cybersecurity in medical devices: guidance for industry and food and drug administration staff”, 23/Mart/2020 tarihinde erişildi, <https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf>
- FDA, (2019), “Cybersecurity Vulnerabilities Affecting Medtronic Implantable Cardiac Devices, Programmers, and Home Monitors: FDA Safety Communication”, 10/03/2020 tarihinde erişildi: <https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-affecting-medtronic-implantable-cardiac-devices-programmers-and-home>
- FDA. (2019), FDA warns patients and health care providers about potential cybersecurity concerns with certain Medtronic insulin pumps, PR Newswire. Retrieved June 28, 2019, 20/04/2020 tarihinde erişildi: <https://www.fda.gov/news-events/press-announcements/fda-warns-patients-and-health-care-providers-about-potential-cybersecurity-concerns-certain>
- Finkle, J., (2016), “J&J warns diabetic patients: Insulin pump vulnerable to hacking”, Reuters Technology News, 15/03/2010 tarihinde erişildi, <https://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e/jj-warns-diabetic-patients-insulin-pump-vulnerable-to-hacking-idUSKCN12411L>
- Freiherr, G., (2017), “The Rising Danger of Cyber Crime in Healthcare”, Imaging Technology News (itn), 10/2/2020 tarihinde erişildi: <https://www.itnonline.com/article/rising-danger-cyber-crime-healthcare>
- HackRead, (2016), “Johnson & Johnson’s Insulin Pumps vulnerable to cyber attacks”, 02/03/2020 tarihinde erişildi: <https://www.hackread.com/johnson-johnsons-insulin-pumps-hackable/>

- HHS, (2020), U.S. Department of Health and Human Services Office for Civil Rights, 11/01/2020 tarihinde erişildi: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
- HIMSS, (2019), "HIMSS Healthcare and Cross-Sector Cybersecurity Report", 28/03/2020 tarihinde erişildi: <https://www.himss.org/resources-himss-healthcare-and-cross-sector-cybersecurity-report?ItemNumber=47762>
- HIPAA, (2019), "2019 Healthcare Data Breach Report", 20/01/2020 tarihinde erişildi: <https://www.hipaajournal.com/2019-healthcare-data-breach-report/>
- HIPAA, (2020), "HIPAA for dummies", 28/01/2020 tarihinde erişildi, <https://www.hipaaguide.net/hipa-a-for-dummies/>
- IBM Security, (2020), "Cost of Data Breach Report 2019", <https://www.ibm.com/security/data-breach>, 04.03.2020 tarihinde erişildi.
- IBM, (2020), "Data security", 1/11/2020 tarihinde erişildi: <https://www.ibm.com/security/data-security>
- Loukas, G., (2015), "Cyber-Physical Attacks: A Growing Invisible Threat", Butterworth-Heinemann.
- Meisner, M., (2017), "Financial consequences of cyber attacks leading to data breaches in healthcare sector", Copernican Journal of Finance & Accounting, volume 6, issue 3.
- Newman, L.H., (2018), "A New Pacemaker Hack Puts Malware Directly on the Device", Wired, 15/03/2020 tarihinde erişildi: <https://www.wired.com/story/pacemaker-hack-malware-black-hat/>
- Pennic, J., (2019) "Quest Diagnostics Confirms 12M Patients Information Exposed in Data Breach", 25/01/202 tarihinde erişildi: <https://hitconsultant.net/2019/06/03/quest-diagnostics-confirms-12m-patients-information-exposed-in-data-breach/#.XnZyRIgzbiU>
- Ozan Özpırlak, B. (2019), "Yapay Zeka ve Hukuk", Sağlık Bilimlerinde Yapay Zeka, Eds. Bulut, M., Dilmen, N., Esmer, G. B., Gezer, M., Selçukcan Erol, Ç., Türker Şener, L., Çağlayan yayınevi, ISBN 9789754361674, sf 231-244.
- Özkan, Y., Erol, Ç.S., (2019), "Kanser Biyoenformatiğinde Yapay Zeka", Papatya Yayıncılık.
- Rai, M., (2016), "Medjacking – An Epidemic in Healthcare", HealthCare IT News, Erişildiği tarih: <https://www.healthcareitnews.com/sponsored-content/medjacking-%E2%80%93-epidemic-healthcare>
- Say, C. (2018). 50 soruda Yapay Zeka, İstanbul: Bilim ve Gelecek Kitaplığı
- Sheridan, K., (2017), "Medjack.3 Poses Advanced Threat To Hospital Devices", DarkReading, 20/01/2020 tarihinde erişildi, <https://www.darkreading.com/endpoint/medjack3-poses-advanced-threat-to-hospital-devices/d/d-id/1328172>
- Silver, E., "Why Are Hackers Targeting Hospitals?", 19/02/2020 tarihinde erişildi: <https://getreferrallmd.com/2019/10/why-are-hackers-targeting-hospitals/>
- Solms, R., Niekerk, J., (2013), "From information security to cybersecurity", Elsevier, Computers & Security, October 2013.
- Staines, R., (2019), "Medtronic defibrillators vulnerable to hacking, says FDA", 20/03/2012 tarihinde erişildi: <https://pharmaphorum.com/digital/medtronic-defibrillators-vulnerable-to-hacking-says-fda/>
- Taylor, H., (2020), "What are cyber threats and what to do about them", Prey, 22/02/2020 tarihinde erişildi: <https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/>
- TechnoExploit, (2018), "What's difference between Tor and VPN, What is Tor and VPN", 20/03/2020 tarihinde erişildi: <https://www.technoexploit.com/2018/07/what-s-difference-between-tor-and-vpn-what-is-tor-what-is-vpn.html>
- Tosun, Y., Gezginci, E., Göktaş S., 2019. "Siber Güvenlik: Sağlık Hizmetleri Ne kadar Güvende?", JAREN, doi:10.5222/jaren.2019.27879. 13/04/2020 tarihinde erişildi: <https://www.journalagent.com/jaren/pdfs/JA-REN-27879-REVIEW-TOSUN.pdf>
- Tully, J.L., Jarrett, M., Savage, S., Corman, J., & Dameff, C.J. (2018), "Digital Defenses for Hacked Hearts: Why Software Patching Can Save Lives", Journal of the American College of Cardiology, 72 1, 126-127.

- Vallance, C., (2015), “Kalp pili hack’lenebilir mi?”, BBC News Türkçe, https://www.bbc.com/turkce/multimedia/2015/12/151203_kalp_pili_hacklenir_mi, 22/03/2020 tarihinde erişildi.
- Whitman,M.E., Mattord,H.J., (2009), “Principles of information security”, (3rd ed.), Thompson Course Technology.
- Wikipedia, (2020), “United States Department of Health and Human Services, Administration for Children and Families. Information Memorandum. 22/03/2020 tarihinde erişildi.