SİBER GELİŞMELERİN SAĞLIK HİZMETLERİNE YANSIMASI VE GÜVENLİK

Büşra Güler[♣]

Özet

Sağlık endüstrisi hastane ve doktor merkezli olmaktan hasta merkezli bir konuma evrilmektedir. Tıbbi cihazların hastane bilgi teknolojileri ağlarına bağlanması hastalar açısından önemli faydalar sağlamaktadır. Hastalar aynı konuda hastane ve doktor değiştirdiklerinde tetkik ve tahlillerin yenilenmesine ihtiyaç kalmamaktadır. Diğer taraftan hastaneye ulaşamamak veya yanlış teşhis ve tedaviyle hasta kayıpları da minimize edilecektir. Elektronik tıbbi kayıt sistemleri daha doğru bakım sağlamaktadır. İnsülin pompaları, kalp atışını düzenleyen defibrilatörler, kalp pilleri, ilaç enjeksiyon pompaları, Manyetik Rezonans Görüntüleme (MR) cihazları, kalp monitörleri hastane bilgisayar ağları içinde yaygın olarak kullanılmaktadır. Bu cihazların sağladığı veriler doktor ve hasta açısından büyük faydalar sağlamaktadır. Gerekli siber güvenlik tedbirleri alınmadığında/alınamadığında büyük zararlara yol açacağı bilinmektedir. Sağlıkta kullanılan birbirine entegre kolay erişim noktaları, eski sistemler, güncellemelerin yetersiz olması saldırılara daha açık hale gelmesine neden olacaktır. Hastane ve hasta bilgileri daha çok fidye amaçlı siber saldırılara maruz kalmaktadır. Kişisel sağlık bilgileri kredi kartı bilgilerinden on kat daha fazla getiri sağlamaktadır. Bu nedenle sağlık hizmetleri ekonomik veya politik getirileri nedeniyle siber saldırılara açıktır. Gelecekte daha fazla saldırı olacaktır ve bunların bir kısmı başarıya ulaşacaktır. Siber güvenliğin önemli hedefleri arasında hasta güvenliği ve özel bilgileri korumak yer alır. Beklenen verimin alınması ve hasta bilgilerinin güvenliği için sağlık teknolojilerine daha fazla yatırım yapılmalıdır. Hastaların sağlıklı ve normal hayatlarını devam ettirebilmeleri üretici ve uygulayıcıların birlikte daha güvenli yazılımlar geliştirmesine bağlıdır.

Anahtar Kelimeler: Sağlık Hizmetleri, Hastane Bilgi Teknolojileri, Siber Güvenlik, Tıbbi Cihaz.

Abstract

The health industry is evolving from being hospital- and doctor-centered to a patient-centered position. Connecting medical devices to hospital information technology networks provides

♣ Ph.D Student, Industrial Engineering, Konya Technical University

important benefits for patients. When the patients change the hospital and doctors on the same subject, there is no need to renew the medical workup and medical analyzes. On the other hand, patient losses will be minimized by not reaching the hospital or by misdiagnosis and treatment. Electronic medical record systems provide more accurate care. Insulin pumps, heart rate regulating defibrillators, pacemakers, drug injection pumps, magnetic resonance imaging (MR) devices, heart monitors are widely used in hospital computer networks. The data provided by these devices provide great benefits for the doctor and the patient. It is known that if the necessary cyber security measures are not taken / cannot be taken, it will cause great damages. Easy access points integrated in healthcare, legacy systems, insufficient updates will make it more vulnerable to attacks. Hospital and patient information is more exposed to ransom cyber attacks. Personal health information returns ten times more than credit card information. Therefore, health services are vulnerable to cyber attacks because of their economic or political benefits. There will be more attacks in the future and some of them will be successful. Important goals of cyber security are patient safety and protecting private information. Further investment in health technologies should be made to achieve the expected efficiency and to secure patient information. The continuation of the healthy and normal lives of the patients depends on the fact that manufacturers and practitioners develop safer software.

Keywords: Health Services, Hospital Information Technology, Cyber Security, Medical Device.

Siberin Gelişimi

İletişimde yeni bir çığır açan bilgisayarlar 1955 yılında dünyanın tamamında 255 civarında iken günümüzde sayıları milyarları geçmiştir (Karakaş, 2016:10). İnternet alışkanlıklarımızda ciddi dönüşümlere neden olmuş, alışverişten seyahate kadar günlük hayatımızın içerisinde sürekli başvurduğumuz önemli yollardan biri haline gelmiştir. Öyle ki internet olmadan yaşamak imkânsız gibi görünmeye başlamış, insanlar mobil cihazlarından ayrıldıklarında kendilerini hayattan kopmuş farz etmeye başlamışlardır (Karakaş, 2016:7-8).

Günümüzde bilgisayar ve internet, tıp alanındaki verimliliği artırmak, hasta ile ilgili bilgileri kaydetmek, değerlendirmek, iletişim sağlamak için vazgeçilmez hale gelmiştir. Tıpta cihazların ağlarla birbirine bağlanması elde edilen bilgilerin akıllı bir şekilde ilgili yerlere ulaştırılması esasına dayanan "endüstriyel internet" sistemi büyük kolaylıklar sağlamaktadır (Karakaş, 2016:5-8).

Veri akışının hızlanması verileri geleneksel yöntemlerle muhafaza ve analiz etme imkânını ortadan kaldırmıştır. Bir kısım riskleri bulunmasına rağmen hasta bilgilerinin bulut sistemi içerisinde muhafaza edilmesi en yaygın yöntemlerden biridir. Depolama hizmetlerinin (bulut sistemi) bilişim hizmetleri sağlayıcılarından alınması kaçınılmazdır. Bulut sistemi depolama maliyetlerini büyük ölçüde azaltmakta sadece ihtiyaç duyduğunuz bilgileri istediğiniz zaman almanıza imkân sağlamaktadır. Bulut sisteminde sizin bilgilerinizin bir başka ülkedeki şahıslar tarafından öğrenilebilme tehlikesi yanında sizin de başkalarının bilgisine ulaşabilme imkanınız oluşabilmektedir. Ancak bulut sistemi dışında da mahrem bilgilerin bilgisayar korsanları tarafından ele geçirilmesi mümkündür. Diğer taraftan bilişim ağının sahibi kimse, bilgilerin tamamına ulaşma imkanı bulunmaktadır (Karakaş, 2016:17-19). Dijital uygulamalar mahremiyet kavramını büyük ölçüde değiştirmiştir. Kişiler açısından mahrem olarak kabul edilen birçok değer kamuya açık hale gelmek zorunda kalmıştır (Yüksel).

Gelinen noktada tıp, sosyal bilimlere daha fazla ihtiyaç duymaya başlamış sağlık sosyolojisi ve hastaların kültürel yapıları öncelikli olarak dikkate alınmaya başlamıştır (Karakaş, 2016:5). Bilgi teknolojileri maliyetlerin düşürülmesi yanında sağlık hizmetlerinin iyileşmesi, yaygınlaşması ve kalitenin yükseltilmesine etki etmektedir (Kotz vd., 2015). İnternetin sağlık hizmetlerinde verimlilikte en az % 20 iyileşme sağlayacağı öngörülmektedir (Karakaş, 2016:9).

Sağlık Alanındaki Siber Uygulamalar

ABD'de yapılan bir araştırmaya göre hemşireler günlük mesailerinin yirmi bir dakikasını ihtiyaç duyulan cihazları aramakla geçirmektedir. 100 bin kişi hastane imkânlarına ulaşamadığı için hayatını kaybetmekte veya engelli hale gelmektedir. Doktorlar günlük mesailerinin iki buçuk saatini hasta ile ilgili verilerin toplanmasına ayırmaktadır. Yılda 98 bin hastada ölümcül hatalar yapıldığı belirtilmiştir. Siber uygulamalar önleyici sağlık hizmetlerine de büyük katkı sağlayacaktır. Oluşturulacak internet ağlarıyla iklim şartlarındaki değişikliğe bağlı olarak ortaya çıkabilecek bir kısım salgın hastalıklara karşı önceden hazırlıklı olması konusunda veriler de oluşturulabilecektir. İnternetin sağlık alanındaki uygulamalarında "makineleri, sistemleri, hastaneleri ve ülkeleri birbirine bağlamak" konusunda sıkıntılar henüz aşılabilmiş değildir (Karakaş, 2016:8-25). Siber uygulamalar sağlıkta maliyetlerin düşmesine ve hizmet kalitesinin artmasına yardımcı olmuştur (Gökrem ve Bozuklu, 2016). Sağlık hizmetlerindeki farklılıkları ortadan kaldırabilmek ve hastaların hizmetlere ulaşabilmesini

sağlamak amacıyla önemli gelişmeler gözlenmektedir. Örneğin cep telefonu büyüklüğündeki ultrason cihazıyla hastanelerden çok uzaktaki bir şahsın filmleri çekilebilmekte, otomatik olarak kaydedilen bilgiler kablosuz internet üzerinden istenilen doktora gönderilebilmektedir. Tıp eğitiminde oluşturulan eğitim modülleri ile görsel ve işitsel materyaller bulut üzerinden ulaşılabilir hale gelmektedir (Karakaş, 2016:29).

Kablosuz iletişim, değişik tehditlere karşı cihazları korumasız hale getirmekle birlikte hastanede kullanılan cihazların büyük ölçüde kablosuz ağlar üzerinden birbiriyle uyumlu hale getirilmesi (Abouzakhar vd., 2017) birbirine bağlı cihazların kullanımının yaygınlaşmasını sağlamıştır (Fu vd., 2017). Sağlık alanında kullanılan cihazlar her geçen gün gelişmekte buna bağlı olarak cihazlar arasındaki bağlantılar da artmaktadır. Bir hastanın başında 10-15 cihazın aynı anda bulunması sıradan bir gelişme haline gelmiştir. Cihazlar arasındaki bağlantı yapılabilecek hataları azaltmak, verimliliği artırmak ve uzaktan takip imkânları sağlamaktadır (Coventry ve Branley, 2018). Türkiye'de Anadolu Kuzey Kamu Hastaneleri Birliği'nde 17 hastane arasında radyoloji ünitelerinin birbirine entegre edilmesi sonucu hastaların sıra bekleme sorunu ortadan kaldırılmıştır. Bilgisayarlı tomografi (BT) cihazlarının birden fazla şehirde birbirine bağlanmasıyla oluşacak ağlar üzerinden daha doğru analiz yapma kabiliyetinin geliştirilmesini ve hastaların değişik merkezlerde aynı işlemi tekrarlatıp yoğun radyasyon almalarının önüne geçilmiş olacaktır (Karakaş, 2016:8-26).

"İnsan hayatı artık internetten kontrol edilebiliyor" örneğin insan vücuduna şekeri sürekli ölçmek için yerleştirilen cihazlar kan değerlerinde ortaya çıkan normal dışı gelişmeleri kaydedip ciddi bir durum varsa doktorla iletişime geçmektedir. Doktor bilgisayar üzerinden kana verilmesi gereken miktarı girdiğinde hasta gelen değeri onaylayınca vücuda insülin enjekte edilmekte hastanın hastaneye gitme zorunluluğu olmamaktadır. Ancak doktorun gönderdiği değere dalgınlıkla bir sıfırı fazla koyması veya cihazın müdahale ile farklı algılama moduna geçmesi sonucu hastayı öldürme riskini göz ardı etmemek gerekmektedir (Aksu vd., 2011:103). Türkiye'de Sağlık Bakanlığı tarafından uygulamaya konulan e-nabız sistemi ile hastalar muayene, tahlil ve tedavilerinin hangi kuruluşta yapıldığına bakılmaksızın tüm sağlık bilgilerine ulaşma imkânı sağlamaktadır. Kişilerin istediği oranda erişim onayı verdiği kayıtlarının hekimlere açılmasıyla teşhis ve tedavi hızı ve kalitesi artmaktadır.

Doktorların hastalardan Manyetik Rezonans Görüntüleme (MR), Bilgisayarlı tomografi (BT), Elektrokardiyografi (EKG) istekleri hastane bilgi sistemi üzerine yerleştirilen karar destek yazılımlarıyla teşhise yönelik hangi tetkikin yapılması gerektiği konusunda doktor uyarılmakta ve hastanın daha fazla radyasyon almasının önüne geçilmektedir. Diğer bir ifade

ile doktora "Sen bu hastaya beyin tomografisi istemişsin. Bu istek ….olası hastalığa teşhise çok yararlı değil, hem de aşırı radyasyon içeriyor. Bunun yerine hastaya MR istemeni öneririm" uyarısında bulunmaktadır. Türkiye'de kullanılan tıbbi görüntüleme cihazlarının monitörlerinin her gün ayarlarının yapılması gerekmektedir. Teknisyenlerin yapması gereken bu işlem zaman zaman yerine getirilemediği için monitörler Japonya'daki bir bulut platformuna bağlanmıştır. Monitörlerin hepsinin her sabah ayarlarının yapılması internet üzerinden bir aksaklığa meydan verilmeden gerçekleştirilmektedir. Türkiye'deki dört hastanedeki dört cihaz Avrupa'daki sekiz ülkeye dağılmış elli dört görüntüleme cihazıyla sürekli haberleşmektedir. Cihazlar filmleri çekilen hastalara yapılan uygulamaları ve verilen radyasyon miktarını birbiri ile karşılaştırmaktadır (Karakaş, 2016:32-34). Bu yolla uygulamada karşılaşılan sorunlar ve tecrübeler paylaşılmakta hizmet kalitesinin artırılması yönünde önemli bir platform oluşturulmaktadır.

Hastaneler interneti tıbbi kayıt işlemlerinde yaygın olarak kullanmaktadır. Oluşturulan hemşirelik istasyonları sayesinde ilaç pompalarının yaptığı işlemler uzaktan kablosuz olarak izlenebilmektedir (Davis, 2017). Amerika'da Los Angeles'ta General Hospital hastanesinde elektronik hemşire sistemi uygulanmaktadır. Hastalar üzerine yerleştirilen aygıtlar aracılığıyla hastanın kan basıncı, ateşi, nefes alma durumu gibi bilgileri merkez kontrol tablosuna aktarılmakta bilgi işlemciler hasta ile ilgili veriler normalin altına inmiş veya üstüne çıkmışsa kontrol tablosunda bulunan hemşire uyarılmaktadır. Hastanın vücuduna yerleştirilmiş olan birçok üniteden gelen bilgiler doğrultusunda canlı hemşireye gerek kalmadan da bir kısım işlemler yapılabilmektedir. Hastanın ateşinin yükselmesi yönünde bilgiler oluştuğunda hastaya bağlı olan enjektörden ateş düşürücü, tansiyonu yüksekse tansiyon düşürücü verilmektedir. Elektronik hemşireler sağlanan gelişmeye rağmen hastaların sargı bezini değiştirecek ve pansuman yapacak seviyeye ulaşmamıştır. Kaldı ki hastalar mekanik bir hemşire yerine canlı hemşireyi tercih etmektedirler. Günün birinde makinelerin hastaların şikâyetlerini dinledikten sonra hafızasındaki çok sayıdaki bilgiye dayanarak hastalık teşhisi koyması ve tedavi yöntemini belirlemesi olası bir gelişme olacaktır (Akman, 2003:194-195).

Sağlık Hizmetlerine Yönelik Tehditler

İnternetin sağladığı gelişmelerin gelecekte ne getireceği bilinmemekle birlikte bilgi paylaşımının sağladığı zarar ve yararların analizinin iyi yapılması gerekmektedir (Karakaş, 2016:43). Dünyada gerçekleşen siber saldırıların büyük bir bölümü sağlık kuruluşlarını tehdit etmektedir (Akyeşilmen, 2018:85). Sağlık hizmetlerinde siber güvenlik öncelikli hedefler

arasında yer almalıdır. Yapılan araştırmalarda sağlık sektöründeki en önemli konulardan birinin güvenlik olduğu vurgulanmaktadır (Kotz vd., 2015). Sağlık hizmetlerinde uygulanan bilgi teknolojileri sistemi saldırılara karşı savunmasız ve oluşabilen sorunları anlık çözme konusunda yetersizdir. Sağlık sisteminde otomasyon ve kayıtların belli noktalarda toplanması konusunda hızlı ilerlemeler sağlanmakla birlikte mahremiyet ve siber güvenlik konusunda diğer alanlarda uygulanan tedbirlerin gerisinde kalınmaktadır (Kotz vd., 2015). Sağlık sektöründeki siber güvenlik sadece hasta verilerinin korunmasıyla sınırlı olmayıp hasta bilgilerinin mahremiyeti ve hastaların güvenliğini de sağlamayı hedeflemelidir.

Sağlık sektörüne yönelik saldırıların arttığı günümüzde güvenlik kavramı verilerin korunmasından daha fazlasını amaçlamakta (Martin vd., 2017-a) gerçekleştirilen saldırılar sistemin güvenlik seviyesinin yükseltilmesi için vesile olmaktadır (Martin vd., 2017-b). Sağlık hizmetlerine yönelik saldırılar daha çok hastane bilgisayar sistemleri üzerinde yoğunlaşmaktadır. Hastane ağına yönelik saldırılar birçok hastayı etkilemekte doktorlara yanlış bilgi gönderilmesine neden olurken tıbbi cihazlar işlevlerini hatalı yapabilmektedir. ABD Sağlık Bakanlığı'nın 2018 yılında yayınladığı raporda kalp pilleri ve insülin pompalarına yönelik saldırıları engellemek amacıyla yeterli tedbirlerin bulunmadığı açıklanmıştır (Siber Savaş Cephesi, 2019). Hastaların güvenliği için etkili siber güvenlik olmazsa olmazdır (Martin vd., 2017-b). Web tabanlı sağlık işletmelerinin yaygınlaşması hasta güvenliğine yönelik risklerin artmasına zemin hazırlamıştır. Kötü amaçlı yazılımlar vasıtasıyla tıbbi kimlik hırsızlığı hastaların sağlık bilgilerinin güvenliğine yönelik geniş çaplı siber saldırılar gündeme gelmiştir. Bulut hizmetlerinin kullanımının artması zararlı yazılımlar marifetiyle yürütülen tehditlerin artışına neden olmuştur (Abouzakhar vd., 2017). Sağlık teknolojilerinde sağlanan gelişmelere rağmen kullanılan cihazların güvenliğinin yeterli olmadığı, hasta bilgilerinin gizliliği ve bütünlüğünün korunamadığı yönündeki endişeler her geçen gün artmaktadır (Coventry ve Branley, 2018).

Siber güvenlik sağlıkla ilgili bilgilerin korunması bütünlüğünün bozulmamasını amaçlar (Martin vd., 2017-a). Siber alandaki gelişmeler insanlara ve kuruluşlara önemli faydalar sağlamakla birlikte bu teknolojiler daha iyi anlaşılıncaya kadar "emniyet, güvenlik ve gizlilik" konuları hakkında daha geniş araştırmalar yapılmalıdır (Davis, 2017). Türkiye'nin de kendi bilgi depolama sistemini oluşturması gerekmektedir.

Kötü amaçlı yazılımlar vasıtasıyla tıbbi kimlik hırsızlığı ile hastaların sağlık bilgilerinin güvenliğine yönelik geniş çaplı siber saldırılar gündeme gelmiştir (Abouzakhar vd., 2017). Her geçen gün akıllı cihazların insan hayatındaki payının artmasına karşın, kişi bilgilerinin gizliliğini korumak zorlaşmaktadır (Davis, 2017). Siber saldırılar virüs kullanılarak şifre çalma, sistemi çökertme, reklam gösterme faaliyetleri olarak karşımıza çıkarken kurtçuklar marifetiyle ağ üzerinden kendi kendine yayılma özelliği bulunan virüse benzer zararlı yazılımlarla zarar vermektedir. Truva atları, bot, botnet, DoS, klavye takipçisi, fidye yazlım, casus yazılım, reklam yazılımı gibi yollarla saldırlar düzenlenmektedir (Akyeşilmen, 2018:76-80). Tüketiciler kullandıkları cihazlar üzerinden hangi bilgilerinin değerlendiğini bilmemektedir. Akıllı telefonlarda ücretsiz olarak uygulanan bir kısım programlar şahıslarla ilgili tüketici davranışlarını açık veya kapalı şekilde toplamakta ve değişik firmalara satabilmektedir (Davis, 2017).

Sağlık hizmetlerinin siber saldırılara karşı dayanıksız olmasının nedenlerinin başında ekonomik nedenlerle yatırım yapılamaması gelmektedir. Diğer bir neden de verilerin korunmasından kimin/kimlerin sorumlu olduğunun açık şekilde belirlenememesinden kaynaklanmaktadır. Zira müdahalenin hızlandırılabilmesi için bilgilere erişimin çok sayıda görevliye açık olmasını zorunlu hale getirmektedir. Erişimin sınırlandırılması zamanında müdahale imkanını sınırlandırabileceğinden tercih edilmemektedir (Martin vd., 2017-a).

Sağlık bilgi sisteminde güvenlik amacıyla uygulanan kimlik doğrulama aşamalarının iş akışını aksatabileceği ve müdahaleyi geciktirebileceği kuşkusu hâkimdir. Yüz tanıma sistemleri, parmak izi gibi yöntemlerin de sağlık personelinin çalışma ortamında genelde eldiven ve maske taktığı bu nedenle uygulama zorlukları çıkardığı, acil durumlarda bilgilere erişimin reddedilmesinin hastaların geciken müdahale nedeniyle ölümüne neden olabileceği ifade edilmektedir (Kotz vd., 2015). Giriş bilgileri ve parolaların istenmeyen kişilerin eline geçmesini engellemek için retina görüntüleme, yüz tanıma, parmak izi uygulamalarını mümkün olan alanlarda hayata geçirmek gerekmektedir. Siber saldırılara karşı alınabilecek etkin tedbirlerden biri de sigortalama yöntemidir (Coventry ve Branley, 2018).

Sağlık sektöründe yaygın olarak kullanılan insülin pompaları, kalp atışını düzenleyen defibrilatörler (kalbin normal dışı atımını tekrar normal kalp ritmine dönmesini sağlayan araçtır), ilaç enjeksiyon pompaları, görüntüleme cihazları, kalp monitörleri vb. araçlar sıklıkla saldırıya uğramaktadır. Bugün bu cihazları kullanmıyor olmuş olmamız bizim güvenlikte

olduğumuz anlamı taşımamaktadır. Kullanılan cihazlar doktorlar ve hastalar açısından önemli faydalar sağlamakla birlikte gerekli güvenlik şartları oluşturulamadığında telafisi mümkün olmayan zararlar oluşturabilmektedir (Siber Savaş Cephesi, 2019). Sağlık alanında bazı saldırılarda geçici kalp pili, insülin pompası vb. ile birden fazla hastanın etkilenme riski bulunmaktadır (Herdem). ABD'de yapılan araştırmalarda defibrilatörlerin siber saldırıyla kontrollerinin ele geçirilebileceği saldırganların cihazın işlevini değiştirebileceği ve hastanın mahrem bilgilerinin elde edilebileceğini ortaya koymuştur (Siber Savaş Cephesi, 2019). Bazı durumlarda saldırılar rastlantı sonucu önlenmektedir. 150'den fazla ülkede bilgisayar sistemini etkileme boyutuna ulaşan virüs yirmi iki yaşındaki bir araştırmacının tesadüfi müdahalesiyle engellenmiştir (Martin vd., 2017-b).

Sağlık cihazlarına insanların yakınındakilerin de müdahale edebileceği bilinmelidir. Laura Hopkin isimli bir kadın münakaşa ettiği nişanlısından intikam almak amacıyla nişanlısının kullandığı insülin pompasının düşük dozlarda insülin vermesi gerekirken yüksek doza ayarlamasıyla cihaz kapanmıştır. Olayın fark edilmesiyle zamanında müdahaleyle hayatı kurtarılmışsa da bluetooth cihazı ile cinayet işlenebileceği ortaya konmuştur (Siber Savaş Cephesi, 2019). Toplumda ünlü kişilerin sağlık kayıtları her dönemde hedef haline gelmiştir (Coventry ve Branley, 2018). Hasta kayıtları ve sağlık hizmetleri gelecekte daha fazla saldırıya maruz kalacak bu saldırılardan bazıları başarılı olacaktır (Martin vd., 2017-b). Sağlık sektöründe gerçekleşecek saldırılar hasta güvenliğini azaltma, sağlık sistemini işlevsiz hale getirmek ve insan hayatını tehdit edecek boyutları olan bir konudur. Diğer bir ifade ile hasta güvenliği ile siber güvenlik ayrılmaz kavramlar haline gelmiştir. Sağlık sektörü sınırlı savunma imkânlarına rağmen büyük veri potansiyeline sahiptir. Sağlık sektöründeki saldırıları yüzde yüz başarısız hale getirmenin bir yöntemi bulunmamaktadır. Ancak risk yönetimi ile zararları azaltmak mümkündür. Yazılımlar güncellenmeli, gizlilik korunmalı ve hasta bilgilerine erişim sınırlandırılmalıdır (Coventry ve Branley, 2018).

Sağlık Sektörüne Yönelik Yapılan Siber Saldırıların Amacı

Dünyanın her tarafında hastalara sunulan hizmetleri iyileştirmek amacıyla sağlık hizmetlerinde dijital teknoloji her geçen gün yaygınlaşmaktadır. Sağlık hizmetleri yumuşak bir hedef ve zengin bir veri potansiyeline sahip olması nedeniyle saldırılara açık hale gelmektedir (Martin vd., 2017-a). Sağlık hizmetleri günümüzde hackerlar tarafından en çok hedef alınan alanlardan biri haline gelmiştir. Sağlık sektörü ekonomik veya politik potansiyeli nedeniyle hackerlar tarafından veya politik aktivistler tarafından daha fazla hedef haline

getirilmektedir. 2015 yılı verilerine göre sağlık verilerine yönelik bilgisayar korsanlığı ilk amaçlardan biri olmuştur (Coventry ve Branley, 2018). Sağlık sektöründe, bankalara yönelik gerçekleştirilen siber saldırılar kadar yoğun saldırı yapılmamakta ise de son dönemde biyoteknoloji ve ilaç sanayine yönelik gizli bilgileri elde etme amacı taşıyan saldırılar yoğunlaşmaya başlamıştır. Bankalara yönelik saldırılarda kişilere ait kart bilgilerini kolaylıkla iptal etmek mümkünken sağlık kayıtlarında şahısların değiştirilemeyecek bilgileri saldırganların eline geçmektedir (Medikal Akademi, 2016-a).

Hastanelere yönelik uluslararası ve devlet destekli gruplar para, veri hırsızlığı ve teknoloji çalınmasını amaçlamaktadır. Dünya üzerinde 2014 yılında siber saldırılardan 500 milyar euro gelir elde edildiği tahmin edilmektedir (Martin vd., 2017-a). Kayıtların elektronik ortamda tutulmasından önce de hasta bilgilerinin ele geçirilme girişimleri mevcutsa da sadece hastane personeliyle sınırlıydı (Coventry ve Branley, 2018). Sağlık kuruluşlarının eski sistemleri kullanıyor olmaları saldırı amaçlı yazılımların işini kolaylaştırmaktadır (Coventry ve Branley, 2018).

Sağlık sektöründe aralarında veri aktarımı yapan medikal makinelerin kullanımı hızla artması tıbbi cihazların iletişim sistemindeki güvenlik risklerini artırmaktadır (Medikal Akademi, 2016-c). Hastanelerde verimliliği artıran bu makineler yapılacak bir saldırı sonucunda bütün hastane faaliyetlerinin durmasına, hasta bilgilerinin başkalarının eline geçmesine ve zarar görmelerine neden olabilmektedir (Medikal Akademi, 2017).

Sağlık bilgileri daha çok şantaj ve bilgilerin başka amaçlarla kullanılarak kazanç sağlanması amacını taşımaktadır (Medikal Akademi, 2016-a). Sağlık hizmetlerine yönelik yapılan saldırılarda ağırlıklı olarak fidye amaçlı şahsi bilgilerin çalınması, tıbbi cihazlara ait veri hırsızlığı, mevcut verileri silmek amacıyla oluşturulan kötü amaçlı yazılımlar, siyasi amaçlarla verilerin geliştirilmesine yönelik çok boyutlu bir yapı sergilemektedir. Kişiler bilgilerinin ifşa edilmesi, silinmesi veya erişiminin engellenmesi ile tehdit edilmekte ve fidye alınmadan ulaşım imkanlarının ortadan kaldırılması esasına dayanmaktadır (Martin vd., 2017-a). Sağlık sektöründe tutulan kayıtların politik bir değeri de bulunması yanında, sağlık hizmetlerine yönelik saldırılar sonucunda elde edilen sigorta bilgileri üzerinden sağlık hizmeti almak ve ilaçları sağlamak amacıyla yaygın olarak kullanılmaktadır. “Bazen tıbbi kayıtlarda banka hesaplarını açmak, kredi temin etmek veya pasaport almak için yeterli bilgi bile bulunmaktadır.” (Coventry ve Branley, 2018).

Siber saldırıların yapılması sonrasında talep edilen fidye ödeninceye kadar bilgi sistemine erişimlerin engellendiği kâğıt üzerinde tutulan kayıtlara geri dönülmek zorunda kalındığı vakalar olmuştur (Davis, 2017). ABD'de gerçekleştirilen bir fidye yazılım sistemi temelli saldırıda hastane ağları ele geçirilip 3,6 milyon dolar karşılığında bilgiler serbest bırakılmıştır (Medikal Akademi, 2016-c). Ancak yeni nesil sağlık çalışanları elektronik kayıt sistemine göre çalışmaya alışık olduklarından bu değişikliğe ayak uyduramamaktadır (Davis, 2017).

Hastanelerde otomatik olarak gerçekleştirilen anti virüs yazılım güncellemesi sonucunda yapılan hata nedeniyle Nisan 2010'da ABD Rhode Island eyaletindeki hastanelere yönelik saldırılar sonucu hastanelerin üçte biri planlanan ameliyatlarını yapamamış, travma geçiren hastalar dışındaki şahıslara acil servislerde hizmet verilmemiştir (Fu ve Blum, 2013). Hastanelerde kullanılan siber sistemlerin büyük verimlilik ve kolaylık sağlaması yanında yazılım kusurları ile hastalara büyük zarar verebilmektedir. 1980'de Therac-25 radyasyon terapi cihazının verilmesi gereken radyasyondan yüz kat fazla uygulama yaptığı görülmüştür (Davis, 2017).

Yetişkin hastalara evde sağlanan uzaktan sağlık hizmetlerinin başarısı dış müdahalelerden uzak bir uygulamaya bağlıdır. Ev ve hastane arasındaki bağlantılar küçümsenemeyecek güvenlik açıkları ortaya çıkarmaktadır. Yine evde elde edilen verilerin hastaların takibi konusunda kritik önemi yanında çevresel tetikleyicilerin (astım) hasta üzerinde etkilerini doğru olarak hesaplayabilmek gerekir. Günümüze kadar görülmemiş olmakla birlikte hastalara yönelik elektronik reçetelerin, kullanım dozlarının veya ilaçların tehlikeli şekilde kötü amaçlı yazılımlarla değiştirilmesi de mümkündür. Yine vücuda yerleştirilen kalp pillerinin, ilaç pompalarının kablosuz ağ üzerinden yaygın şekilde değiştirilmesi halinde ortaya çıkabilecek sonuçları hayal etmek dahi mümkün değildir (Davis, 2017).

Alınabilecek Tedbirler

Siber riskler "tehdit, güvenlik açığı ve etki" unsurlarına sahiptir (Martin vd., 2017-b). Tıbbi cihazlara yönelik siber tehditler gelişerek artmaktadır. Hastane ağlarına karşı gerçekleştirilen saldırılar hasta güvenliğini ileri derecede etkilemektedir (Kahraman). Bilgisayar dünyasıyla doğrudan alakası olmayan şahısların bile zamanlarının büyük bir bölümü siber alanda geçmektedir. Saldırıya uğrayanlar karşı karşıya kaldıkları tehlikeyi dahi anlayamamaktadırlar (Akyeşilmen, 2018:69). Siber güvenlik konusunda müdahaleye niyetli zeki şahısların ne

yapabileceği, hangi tedbirlerle hızlı ve esnek önlemler alınabileceğini ciddi bir şekilde düşünmemiz gerekmektedir. Saldırganlar sağlık hizmetlerindeki siber uygulamaların giderek artması nedeniyle saldırı yüzeyi de arttığından daha etkili olabilmektedirler. Sağlık sektöründe kullanılan cihazların fiziksel güvenliği konusunda ciddi tedbirler alınmakla birlikte yatırım aşamasında bu cihazlara yönelik siber saldırılar konusunda gerekli uygulamalar ele alınmamıştır (Davis, 2017).

Bağlantı sayısının artması siber güvenlik risklerini artırmaktadır. Dışarıdan saldırı olmasa bile kazayla da bilgilerin aktarılmasında hatalar ortaya çıkabilmektedir (Coventry ve Branley, 2018). Hastanelerde bilgi teknolojilerine bağlı cihazların artması hastaların hayat kalitesinin artırılmasına büyük katkı sağlamaktadır. Ancak hastaların ve sağlık sektörü çalışanlarının kullandıkları 15 milyona yakın cihaz büyük siber güvenlik tehditlerini artırmaktadır (Kahraman). Günümüzde yaygınlaşan monitör uygulamaları kullandığı yazılım açısından hasta güvenliğini sağlayabilecek seviyede değildir. Sağlık hizmetlerinde kullanılan cihazların gelecekte ortaya çıkabilecek tehditlere karşı da savunma seviyelerinin yükseltilmesi ve gelişen tehditlere karşı yeni cihazların tasarlanması gerekmektedir. Sağlık bilgi teknolojileri tasarımcıları kullanılmaya başlayan cihazlara uygun özel güvenlik uygulamaları oluşturarak bilgilerin nerede depolanacağı, kimlerin kullanabileceği ve nasıl kullanılacağı yolunda programlar geliştirerek hasta haklarını koruyan uygulamaları hayata geçirebilirler. Cihazlarda uygulanan yüz tanıma, kimlik doğrulama gibi yeni güvenlik önlemleri uygulamaya geçirilmiş olmakla birlikte insan faktörünün kritik bir rol oynadığı ve uygulayıcıların sık aralıklarla eğitilmesi gerektiği de bir gerçektir (Kotz vd., 2015).

Periyodik yedekleme yaparak ve şifreleri güncelleyerek riskler bir ölçüde azaltılabilir. Siber saldırılara karşı riskleri minimize etmek için alt yapıya ve insana uzun vadeli yatırım yapmak gerekmektedir (Martin vd., 2017-b). Tıbbi cihazlar çok gelişmiş olmasına rağmen koruma sistemleri ihmal edilmiştir (Davis, 2017). Güvenliğin artırılması için cihazların tasarım aşamasından itibaren mühendislerle yazılımcıların güvenlik riskini minimuma düşürecek tedbirleri içeren ortak çalışma gerçekleştirmesi gerekmektedir (Medikal Akademi, 2016-c). Sağlık bilgi teknolojileri yazılımcıları, kullanıcılar ve tıbbi cihaz üreticilerinin işbirliği içerisinde çalışması, tehdit bilgilerinin paylaşılması, zamanında müdahale edilmesi ve güvenlik açıklarının kapatılması açısından önemli olacaktır (Kahraman).

Tıbbi cihaz üreticileri tasarım aşamasından itibaren siber güvenlikle ilgili tedbirleri göz önünde bulundurmalıdır. Tıbbi cihaz güvenliğindeki hacker girişimler sağlık güvenliğinin ancak bir kısmını ifade etmektedir. Kullanıcılar karşılaştıkları güvenlik açıklarını bildirmeye yönelik teşvik edilmelidir (Fu ve Blum, 2013). Siber saldırılara maruz kalan cihazların geri çağrılmasına yönelik tedbirler alınmalı, saldırıları rapor etmeye yönelik özendirici suçlama amacı taşımayan uygulamalar hayata geçirilmelidir (Siber Savaş Cephesi, 2019).

Sağlık kuruluşları sistemlerin kullanımından sorumlu tutulmalıdır ve hastanelerdeki bilişim teknolojileri uygulamaları konusunda uzman kuruluşlar tarafından denetlenmeli ve desteklenmelidir (Kotz vd., 2015). Amerika Gıda ve İlaç Dairesi (FDA) tıbbi cihazların üretim aşamasında siber güvenlikle ilgili tedbirlerin alınması ve piyasaya sürüldükten sonra da yayınlanacak "siber güvenlik malzeme listesi" ile muhtemel tehditlere açık cihaz parçalarının belirtilmesini zorunlu hale getirmiştir (Herdem).

Denetim kayıtlarının tıbbi sistemlerinde anlık analiz edilmesi kullanıcı hataları veya sistemden kaynaklanabilecek ayar değişikliklerinin anında müdahale için kontrol altına alınması gerekmektedir. Sağlık hizmetlerinde kullanılan teknolojilere hastaların daha yaygın şekilde kabul etmeleri için şahıslara ait bilgilerin gizliliğinin korunması konusunda insanlara daha fazla güvence verilmesi ve güvenlik önlemlerinin artırılması gerekmektedir (Kotz vd., 2015). Her türlü tehdide karşı tedavi hizmetlerinin devam edecek şekilde planlanması, güvenlik risklerinin ve gizliliğinin öncelikli amaçlar arasına alınması, saldırılara karşı tıbbi cihazların dayanıklılığının artırılması gerekmektedir (Fu ve Blum, 2013).

Kullanılan platformlarda yüksek seviyede şifreleme sistemleri kullanılmakla birlikte dışarıdan müdahale edilmeye her zaman müsaittir. Bunların önüne geçebilmek için mümkün olduğu oranda ulusal sistemlerin oluşturulması gerekmektedir. Mahrem bilgilerin güvenlik seviyelerinin yüksek olduğunu ancak başka şirketlerin hizmetine bağlı olduğunuz anda yeteri kadar güvenilir olmayacaktır. Dünyanın önde gelen şirketlerinin sağladığı bilgi depolama yöntemlerinde ileri teknolojiye dayanan güvenlik tedbirleri alınmaktaysa da mutlak bir güvenliğin sağlanamayacağı da aşikârdır. Diğer bir ifade ile mükemmel bir şifreleme düşünülmemektedir (Karakaş, 2016:20-37).

Tıbbi cihazlara yönelik saldırılara karşı alınabilecek tedbirler arasında kalp pillerindeki kablosuz bağlantı fonksiyonlarının kaldırılması, kullanılan cihazların yazılım

güncellemelerinin sürekli yapılması, hastalara sıvı enjekte eden cihazların daha dikkatli kullanılması, radyolojik görüntüleme cihazlarının güvenlik kontrollerinin artırılması önerilmektedir (Siber Savaş Cephesi, 2019). Sağlık personelinden güvenli olmayan cihazlardan güvenli veriler oluşturması istenmektedir. Finansal problemler nedeniyle cihazlardaki yazılımların güncellenememesi veya tamir edilemeyen cihazların kullanılmaya devam edilmesi oranında riskler artmaktadır (Fu ve Blum, 2013). Doktorlardan biri güvenlik uzmanlarına "güvenlik ihtiyacınızın hastalarımdan birini öldürdüğü günden korkuyorum" (Kotz vd., 2015) ifadesi tehlikenin bilinmezliğini ortaya koymaktadır.

Sonuç

Sağlık hizmetlerini tehdit eden faktörler arasında siber saldırılar önemli bir yer tutmaktadır. Siber saldırılar ekonomik kayıplara, itibar kaybına ve hastaların güvenliklerine zarar vermektedir. Siber güvenlik hasta bilgilerinin korunması ve hasta güvenliğinin sağlanması açısından kritik bir önem taşımaktadır. Hedefe ulaşabilmek için daha fazla para ve çalışma gerekmektedir. Güvenlik önlemleri cihazların tasarım aşamasında ele alınmalı ve siber güvenlik sağlık hizmetleri kültürünün kritik bir parçası olarak düşünülmelidir. Siber güvenlik hasta bakım kültürünün önemli bir parçası olmalı ve uygun olmayan güvensiz süreçler daha güvenli yaklaşımlarla değiştirilmelidir (Coventry ve Branley, 2018).

Hastanelerde kullanılan tıbbi cihazların siber saldırıya uğraması yaygın bir olay haline gelmiştir. Bir cihaza yapılacak saldırı ona bağlı bütün cihazları risk altında bırakmaktadır. Günlük hayatımızda kullandığımız teknolojik gelişmelerin önemi arttıkça hasta bilgilerinin farklı kaynaklara ağ üzerinden aktarılması maruz kalınabilecek riskleri ve şiddetini artırmaktadır (Medikal Akademi, 2017). Sağlık hizmetlerinin çok iyi bir seviyeye ulaşsa bile sağlık hizmetlerini tehdit eden faktörlerin ortadan kaldırılamadığı müddetçe riskler önemli bir çalışma alanını oluşturacaktır (Yeni Şafak, 2018).

Tıbbi cihazlar arasındaki iletişimde emniyet, güvenilirlik, sağlamlık ve esneklik özeliklerine itina gösterilmelidir. Günümüzde tıbbi cihazlar kişiye özel tıbbi uygulamalardan eczacılığa, hastalık teşhisine ve hasta bakım hizmetlerine kadar geniş bir alanı etkileyen yazılımlara dayanmaktadır. Kötü amaçlı yazılımlar tıbbi cihazların işletim sistemlerini etkileyerek fonksiyonlarını yerine getirmesini engellemektedir. Kötü yazılımların etkili olduğu durumlarda hastalar istenilen seviyede tedavi hizmeti alamamaktadır (Fu ve Blum, 2013). Sağlık sektöründe kullanılan cihazların her birinin bağlantı alanları ve işlevleri dikkate

alınmalıdır. Öyle ki sadece doğrudan sağlıkla ilgili cihazlar dışında, güç kaynakları veya su sistemine yapılabilecek bir siber saldırı hastaların tedavisine yönelik çalışmaları büyük ölçüde etkileyebilir (Davis, 2017). Siber güvenliğin sağlanması sadece teknik ve politik konu olmayıp bu alanda faaliyet sürdüren bütün birimlerin iş birliği yapması halinde kısmen başarılı olabilir (Akyeşilmen, 2018:110).

Türkiye'de sağlık kuruluşlarının bilgileri çok güvenli olduğu düşünülen sağlık bilişim ağına bağlanmakla birlikte 33 kamu hastanesine yönelik aynı anda başlatılan saldırılardan Diyarbakır ilindeki bazı hastaneler etkilenmiştir. Saldırının zamanında fark edilmesiyle yedeklemenin güncellenmesi veri kayıplarını önemli ölçüde engellemiştir (Medikal Akademi, 2016-b).

Sağlık Bakanlığı'nın Amerikalı Anonymous hacker grubunun 33 hastaneye yaptığı saldırıda bilgilerin korunduğunu duyurmasına rağmen hastalara ait aids, hepatitb ve diyabet gibi sağlık bilgilerinin Youtube üzerinden yayınlanmış olması saldırının başarısız olduğu iddialarını çürütmektedir. Saldırıya uğrayan sağlık verilerinin Yapılandırılmış Sorgu Dili (SQL) dosyası olarak korunuyor olması büyük bir hata olarak değerlendirilirken 50 milyondan fazla insanın kimlik bilgilerinin de elde edilmesi Türkiye'deki veri güvenliğinin zaaf içerisinde olduğunu göstermiştir. Hackerlar Türkiye'den intikam almak için bunu yaptıklarını açıklayarak benzeri saldırıların hangi amaçlara hizmet edeceğini de pek düşünmediklerini göstermektedir (Kandemir, 2017).

Nesnelerin interneti mobil dijital medikal uygulamaların yaygınlaşmasını sağlamıştır. Sensor ağları vücut hakkındaki birçok fizyolojik veriyi anlık toplayıp hasta hakkındaki değişiklikleri istenen merkeze iletmektedir. Ancak internet erişimi kesilirse ne olacak? (Nesnelerin İnterneti ve Endüstriyel Uygulamaları) sorusu henüz yeterince gündem oluşturmamıştır.

Türkiye tıbbi cihazlara yönelik tehditleri dikkate almak sureti ile yüksek teknolojiye sahip cihazların ülkemiz imkânlarıyla üretilmesine yönelik ulusal bir politika oluşturma gayreti içerisine girmiştir (Yeni Şafak, 2018). Ancak sisteminizin kendinize ait olması da güvenliğinizin tam olduğu anlamını taşımamaktadır. Türkiye'deki Sosyal Güvenlik Kurumu'na gönderilen veriler her coğrafyadan ulaşılabilir. Güvenlik kodlarında uygulanan yan kapı sistemlerin birbirine entegre olması nedeniyle diğer alanlara ulaşmayı mümkün

kılmaktadır. Örneğin e-devlete bir yerden girdikten sonra kişilerle ilgili birçok işlemi yapabilmek mümkün hale gelebilmektedir (Karakaş, 2016:38).

Hastaneler hassas bilgilere erişimi engellemek amacıyla daha karmaşık kimlik doğrulama mekanizmaları oluşturmalıdır. Sağlıkla ilgili bulut hizmetlerine yönelik karmaşık kimlik doğrulama yetkilendirme aşamaları uygulanmalıdır (Abouzakhar vd., 2017). Siber alanda güvenlik hiçbir dönemde yüzde yüz sağlanamayacak ve sağlık hizmetleri de saldırılardan etkilenecektir. Saldırılardan büyük ölçüde etkilenmemek, en azından bilgiler çalınsa bile kaybolmasını engellemek amacı ile güncel yedeklemeler yapılmalıdır. Saldırılara karşı alınabilecek etkili yöntemlerden biri de sigortalatma sistemidir. Sigorta işlemi devreye girdiğinde güvenlik standartlarının artırılmasına yönelik ciddi bir gayret içerisine girilecektir. Günümüzde ise sağlık sektöründe siber saldırılara karşı oluşturulmuş standart bir koruma önlemi bulunmamaktadır (Martin vd., 2017-a).

Kaynaklar

Abouzakhar, N.S., Jones, A., Angelopoulou, O. (2017). Internet of Things Security: A Review of Risks and Threats to Healthcare Sector. IEEE International Conference on Internet of Things, Exeter, UK.

Akman, T. (2003). Sibernetik Dünü, Bugünü, Yarını. İstanbul: Kaknüs Yayınları.

Aksu, H., Candan, U., Çankaya, M.N. (2011). Her Şey Çıplak Bildiğiniz İnternetin Sonu: Web3 3.0. İstanbul: Kapital Medya Hizmetleri.

Akyeşilmen, N. (2018). Disiplinlerarası Bir Yaklaşımla Siber Politika ve Siber Güvenlik. Ankara: Orion Yayınları.

Coventry, L., Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Elsevier Maturitas 113 (2018) 48–52.

Davis, J. (2017). TheLighter Side of Things: The Inevitable Convergence of the Internet of Things and Cybersecurity, Information Technology ve CIO NASA Ames Research Center GITEC.

Fu, K., Blum, J. (2013). Inside Risks, Controlling for Cybersecurity, Risks of Medical Device Software. Communications Of The Acm October 2013, Vol. 56, No. 10.

Fu K., Kohno T., Lopresti D., Mynatt E., Nahrstedt K., Patel S., Richardson D., Zorn B., (2017). Safety, Security, and Privacy Threats Posed by Accelerating Trends in the Internet of Things. http://cra.org/ccc/resources/ccc-led-whitepapers/.

Gökrem, L., Bozuklu, M. (2016). Nesnelerin İnterneti: Yapılan Çalışmalar ve Ülkemizdeki Mevcut Durum. Gaziosmanpaşa Bilimsel Araştırma Dergisi. Sayı: 13, Sayfa:47-68.

Herdem. (10 Aralık). FDA Tıbbi Cihazların Siber Güvenliği için Harekete Geçti. http://herdem.av.tr/tr/fda-tibbi-cihazlarin-siber-guvenligi-icin-harekete-gecti/. Erişim Tarihi: 09.06.2019.

Kahraman, H. Akıllı Tıbbi Cihazların Siber Güvenliği. https://www.endustri40.com/akilli-tibbi-cihazlarin-siber-guvenligi/. Erişim Tarihi: 09.06.2019.

Kandemir, H. (2017). Hacker grubu Anonymous, Türkiye'deki sağlık bilgilerini hackleyip yayınladı. https://www.medikalakademi.com.tr/hacker-grubu-anonymous-tuerkiyedeki-tuem-saglik-verilerini-hackledi/. Erişim Tarihi: 10.06.2019.

Karakaş, M., H. (2016). Büyük Veri, Endüstriyel İnternet ve Sağlık Alanındaki Uygulamaları. Betim Konferansları. (Editör: Hakan Ertin). Hayat Sağlık ve Sosyal Hizmetler Vakfı, Beşikcizade Tıp ve İnsani Bilimler Merkezi.

Kotz, D., Fu, K., Gunter, C., Rubin, A. (2015). Privacy and Security, Security for Mobile and Cloud Frontiers in Healthcare, Communications of the ACM, August 2015, Vol. 58 No. 8, Pages 21-23.

Martin, G., Martin, P., Hankin, C., Darzi, A., Kinross, J. (2017-a). Cybersecurity and healthcare: how safe are we?. BMJ 2017;358:j3179 doi: 10.1136/bmj.j3179.

Martin, G., Kinross, J., Hankin, C. (2017-b). Effective cybersecurity is fundamental to patient safety. The NHS must reduce its vulnerability and build resilience against future cyber attacks. BMJ 2017;357:j2375 doi: 10.1136/bmj.j2375.

Medikal Akademi. (2016-a). Siber Suç Ekonomisi Sağlık Sektöründeki İyi Korunmayan Verileri Hedef Alıyor. https://www.medikalakademi.com.tr/siber-suc-ekonomisi-saglik-sektoruendeki-iyi-korunmayan-verileri-hedef-aliyor/. Erişim Tarihi: 10.06.2019.

Medikal Akademi. (2016-b). Sağlık Bakanlığı'ndan hastanelere yapılan siber saldırı ile ilgili açıklama. https://www.medikalakademi.com.tr/saglik-bakanligi-hastane-siber-saldiri-aciklama/. Erişim Tarihi: 10.06.2019.

Medikal Akademi. (2016-c). Siber korsanların gözü sağlık sektöründe ve hastanelerde. https://www.medikalakademi.com.tr/siber-korsanlarin-gozue-saglik-sektoruende-ve-hastanelerde/. Erişim Tarihi: 10.06.2019.

Medikal Akademi. (2017). Akıllı tibbi cihazlar siber tehdit altında sağlık verileriniz güvende mi. https://www.medikalakademi.com.tr/akilli-tibbi-cihazlar-siber-tehdit-altinda-saglik-verileriniz-guevende-mi/. Erişim Tarihi: 10.06.2019.

Nesnelerin İnterneti ve Endüstriyel Uygulamaları, http://www.endustri40.com/nesnelerin-interneti-ve-endustriyel-uygulamalari/, Erişim Tarihi: 10.04.2018.

Siber Savaş Cephesi. (2019). Medikal Cihazların Hacklenmesi Yalnız Hastaneleri İlgilendirmiyor. https://sibersavascephesi.com/2019/03/27/medikal-cihazlarin-hacklenmesi-yalniz-hastaneleri-ilgilendirmiyor/. Erişim Tarihi: 09.06.2019.

Yeni Şafak. (2018). Sağlıkta hedef yüksek teknolojili tıbbi cihaz imalatı. https://www.yenisafak.com/hayat/saglikta-hedef-yuksek-teknolojili-tibbi-cihaz-imalati-3410231. Erişim Tarihi: 09.06.2019.

Yüksel, Y.S.S. Nesnelerin İnterneti (İnternet of Things) ve Değerler, http://www.bs.org.tr/blog/nesnelerin-interneti-internet-of-things-ve-degerler/41, Erişim Tarihi: 10.04.2018.