JAREN
doi:10.5222/jaren.2019.27879

Derleme / *Review*

Siber Güvenlik: Sağlık Hizmetleri Ne kadar Güvende?

Cyber Security: Are Healty Services Reliable?

Yıldız TOSUN[1], Elif GEZGİNCİ[2], Sonay GÖKTAŞ[2]

[1]*Taksim Eğitim ve Araştırma Hastanesi, İstanbul, Türkiye*
[2]*Sağlık Bilimleri Üniversitesi, Sağlık Bilimleri Fakültesi, Cerrahi Hastalıkları Hemşireliği Anabilim Dalı, İstanbul, Türkiye*

ÖZ

Amaç: *Sağlık bakım hizmetlerinin sunumunda bilişim teknolojileri yaygın olarak kullanılmaktadır. Kaliteli ve güvenli bir bakımın sağlanmasında bilişim teknolojilerinin önemi büyüktür. Bilişim teknolojisi; bilgi yönetimi, paylaşımı ve kolay erişimi sağlayarak bakım güvenliğini büyük ölçüde sağlamaktadır. Bilişim teknolojilerinin sağladığı bu olumlu özelliklerin yanı sıra her cihazın uzaktan kontrol edilebilir ve ulaşılabilir olması sağlık verileri ve cihazların güvenliği ile ilgili endişelere yol açmaktadır. Sağlık sektörü, zengin veri kaynaklarına sahip olması ve korumaya yönelik savunmalarının az olmasından dolayı siber suçlular tarafından çekici hale gelmektedir. Hastanelerdeki siber tehdit sağlık bilgileri ve hastanelere yapılan fidye saldırıları dışında aynı zamanda tıbbi cihazlara ve altyapıya yönelik saldırıları da içermektedir. Sağlık hizmeti veren kuruluşlarda siber güvenliğe yönelik yeterince önlem alınmaması hasta güvenliğini tehlikeye sokabilmektedir. Siber güvenlik hasta güvenliğinde kritik öneme sahip olmasına rağmen gelişen teknoloji ile birlikte güvenlik önlemlerinin artırılmasını gerekli kılmaktadır. Sonuç olarak siber güvenlik hasta güvenliğinin ayrılmaz bir parçası haline gelmiştir. Bu makalede sağlık bakım hizmetlerinin sunumunda hasta güvenliğini tehdit eden siber güvenliğin önemi vurgulanmış olup, güvenlik önlemlerinin artırılmasına yönelik daha fazla çalışmanın yapılması gerektiğine değinilmektedir.*

Anahtar kelimeler: *Siber güvenlik, bilişim, hasta güvenliği*

ABSTRACT

Objective: *Information technologies are widely used in the presentation of health care services. Information technologies are important in providing quality and safe maintenance. Information Technology provides a large degree of maintenance security by providing information management, sharing and easy access. In addition to these positive features provided by information technologies, the fact that each device can be remotely controlled and accessible causes concerns about health data and the safety of devices. The health sector is attractive by cyber criminals because of its rich data sources and low defense defenses. Cyber threats in hospitals include health information and ransom attacks on hospitals, besides attacks on medical devices and infrastructure. Failure to take adequate measures for cyber security in healthcare organizations may endanger patient safety. Although cyber security is critical in patient safety, it is necessary to increase security measures with developing technology. As a result, cyber security has become an indivisible part of patient safety. In this article, the importance of cyber security that threatens patient safety is emphasized in the presentation of health care services and more studies are needed to increase the security measures.*

Keywords: *Cyber security, informatics, patient safety*

Yazışma adresi: Hemşire Yıldız Tosun,
Karayolları Mahallesi, Osmanbey Caddesi 621. Sokak
Gaziosmanpaşa 34255 İstanbul - Türkiye
e-posta: yildiztsn@hotmail.com

ORCID
Y.T. 0000-0003-1002-472X
E.G. 0000-0003-0392-5298
S.G. 0000-0002-8168-1287

Alındığı tarih: 10.07.2019
Kabul tarihi: 28.10.2019

GİRİŞ

İnsanlık, bilinen tarihi boyunca sürekli bir değişim içerisindedir. Sanayi devriminden beri yaşam tarzının iyileştirilmesine katkıda bulunan çeşitli teknolojiler geliştirilmiştir. Bunların en önemlisi 1900'lü yılların sonuna doğru ortaya çıkan ve bugün 2,3 milyar kişinin kullandığı internettir [1,2]. İnternetin yaygın olarak kullanılmaya başlanması ile coğrafi sınırlılıklar ve zaman kısıtlamaları ortadan kalkmış, insanların her türlü elektronik bilgiye erişimi sağlanan yeni bir dünya oluşmuştur [3]. Bu yeni dünyada bugün küresel ağ üzerinde 4,021 milyar internet kullanıcısı, 3,196 milyar aktif sosyal medya kullanıcısı, 5,135 milyar mobil telefon kullanıcısı ve 2,958 milyar aktif mobil sosyal medya kullanıcısı bulunmaktadır [4]. Türkiye İstatistik Kurumu'nun 2017 yılında yayınladığı rapora göre Türkiye'de internet erişimi %95,9 bilgisayar kullanımı %97,2 olup bu bilgisayarların neredeyse tamamının internet bağlantısına sahip olduğu saptanmıştır [5]. 1960 yılında ortaya çıkan internetin çıkış amacı bilgi paylaşmaktır. Fakat günümüzde internet kullanımının bu kadar yaygınlaşacağı tahmin edilmediği ve insanların sisteme zarar verebilecekleri düşünülmediği için güvenlik geri planda kalmıştır [1]. 21. yüzyılda bilgi ve iletişime dayalı teknoloji kendini tehdit edebilecek oluşumları da beraberinde getirmiştir [6].

Siber Güvenlik

Sibernetik kelime kökünden türetilen siber sözcüğü, bilişim ve iletişim ağlarının oluşturduğu uzayı ifade etmektedir [3]. Siber sözcüğünün ilk olarak 1958 yılında Sibernetik biliminin babası olarak tanınan Louis Couffignal tarafından kullanıldığı belirtilmektedir [7]. Siber güvenlik ise bilgi güvenliği (information security) ve bilgisayar güvenliği (computer security) kavramları ile benzer anlamlarda kullanılmaktadır [8,9]. Siber güvenlik, siber uzayı oluşturan bilgi teknolojileri sistemlerinin tehditlerden korunması, buradaki bilginin gizlilik, bütünlük ve erişilebilirliğinin güvenli bir şekilde sağlanması, saldırı ve siber durumların belirlenmesi, bu belirlemelere yönelik önlemlerin alınması ve sonrasında sistemlerde karşılaşılan sorunların siber güvenlik saldırısı öncesine geri getirilmesi olarak tanımlanmaktadır [10]. Siber güvenliğin ana unsuru bilgidir [8]. Siber uzayın güvenli olabilmesi için bilginin gizliliği (confidentiality), bütünlüğü (intergrity) ve erişilebilirliğinin (availability) sağlanması gerekmektedir [8,11].

Siber Güvenliğin Önemi

21. yüzyılda bilim ve teknoloji alanındaki ilerlemeler güvenliğin yeni boyutlarının ortaya çıkmasına neden olmuştur [12]. Günümüzde neredeyse tüm bilgi siber ortamda depolanıp işlenmekte, cihazlar siber ortamda yönetilmektedir. Orduların gücü elektronik haberleşme, görüntü alma, uzaktan algılama gibi yöntemlere dayanmaktadır. New York ve Washington'da 11 Eylül 2001 günü yolcu uçaklarını çeşitli hedeflere çarptırarak yapılan terör saldırıları ile tehdit konusundaki geleneksel anlayış terk edilmiş; kara, deniz, hava ve uzayın yanı sıra beşinci savaş alanı olan siber ortama göre saldırı düzenlenmiştir [3]. Bu saldırılar ile tehdidin açık bir "gönderici adresi" olmadığı, hemen hemen her şeyin her an silaha dönüşebileceğini ve hiçbir şeyin imkânsız olmadığı ortaya konulmuştur [3,12]. Yaşanan değişim süreci ile birlikte güvenlik kavramının herkesin üzerinde anlaşabileceği sınırlarını ve çerçevesini ortaya koymak gittikçe zorlaşmıştır [12]. Siber güvenliğini iş yerindeki bilgisayarlar, tabletler, cep telefonları, dizüstü bilgisayarı ve internet hattı gibi sayısız makine oluşturmaktadır. Siber güvenlik, "tüm bilgisayar ağlarını ve onların bağlı olduğu ve kontrol ettiği her şeyi kapsamaktadır" O halde bilişim teknolojilerini kullanan her birey, siber güvenliğin bir unsurudur [2].

Siber saldırı türleri sayısının çok fazla olmasının yanı sıra giderek yeni saldırı türleri de ortaya çıkmaktadır [13]. Siber saldırı türlerini şöyle sıralayabiliriz [7]:

1) Bilgi ve istihbarat sağlamak için kullanılan casus yazılımlar aracılığıyla yapılan saldırılar,
2) Portal ve internet hizmetinin aksatılması veya engellenmesine yönelik yapılan saldırılar,
3) Yemleme (phishing) olarak adlandırılan ve yasadışı yollardan yanıltma amacıyla yapılan saldırılar,
4) İstem dışı elektronik posta olarak adlandırılan "Spam" yöntemiyle zararlı dosyalar göndererek yapılan saldırılar,
5) Ağ trafiğini dinleyerek yapılan saldırılar,
6) Sosyal medya kullanarak yapılan saldırılar,
7) Sosyal mühendislik,
8) Arama motorları kullanarak yapılan saldırılar,
9) Ücretsiz web hizmeti sunarak yapılan saldırılar.

Siber Güvenlik ve Sağlık Hizmetleri: Ne kadar Güvendeyiz?

Teknoloji ve iletişim alanında yaşanan devrim sonucunda bilgisayar ağları yoluyla bilgiye ulaşma kolaylaşmıştır. Bunun sonucunda; iş hayatına bilgisayar ve bilgi teknolojileri girmesiyle uygulama alanında yeni süreçler ortaya çıkmıştır. Sağlık alanında her gün yeni bilgiler ve uygulamalar arttığı, sağlık kurumları bilgi tabanlı bir topluluk haline geldiği için bu değişimin yaşandığı alanların başında sağlık sektörü gelmektedir. Bu durum, sağlık kurumlarında bilişim teknolojilerinin kullanımını zorunlu kılmış ve günümüzde birçok hastanede hizmet kalitesinin artırılması için bilişim teknolojilerinin kullanımı yaygınlaşmıştır [14]. Elektronik sağlık kayıtları, monitörler, akıllı cihazlar ve teletıp teknolojileri sağlık teknolojilerini oluşturup, sağlığı koruma, geliştirme ve yaşam süresini uzatma potansiyeline sahiptirler [15]. Sağlık hizmetlerinde ihlaller, sağlık sektörü için artan bir tehdittir [16]. Amerika Birleşik Devleti Adalet Bakanlığı tarafından yayınlanan raporda; sağlık sektörünün dünya çapında fidye yazılımdan en çok etkilenen ilk üç sektör arasında olduğu, fidye yazılımının yanı sıra, son iki yılda kötü amaçlı bilgisayar yazılımı saldırılarının sayısının dört kat arttığı ve sağlık sektörünün küresel olarak en çok hedeflenen sektörlerden biri haline geldiğini belirtilmiştir [17].

Sağlık hizmetlerinde yaygın olarak ortaya çıkan siber tehditler [18]

- Finansal kazanç için veri hırsızlığı: Parasal kazanç amacıyla isimler, adresler, sosyal güvenlik detaylar, finansal bilgiler vb. kişisel verileri çalmak,
- Hassas tıbbi bilgilerin çalınması ve kamuya açıklanması: Örneğin ünlüler, politikacılar veya diğer yüksek profilli insanların tıbbi bilgilerini yayınlamak,
- Fidye yazılımı: Bir ücret ödenmediği sürece kullanıcılarının verilerine ulaşımını veya sisteme erişimini engellemek ya da verileri silmek için kötü amaçlı yazılım kullanmak,
- Veri bozulması: Siyasi veya kişisel kazanç için test sonuçlarını değiştirme gibi verilerin kasıtlı bozulması,
- Hizmet reddi saldırıları: Şantaj, intikam veya eylem ile harekete geçerek gereksiz talepler ile bir ağ ya da sistemin işleyişini durdurma,
- İş e-posta uyumu: Finansal kazanç için sahte kişisel hesap oluşturma,
- Çalışanların Kasıtsız eylemleri: Personelin kasıtsız eylemleri ve risk altındaki sistemler nedeniyle veri kaybı ya da sistemlerin ciddi şekilde bozulmasıdır.

Sağlık hizmetleri diğer sektörlerden daha fazla siber risklerle karşı karşıyadır. Siber saldırıları gerçekleştirenler için sağlık sektörünün iki basit ve çekici hedefi vardır. Bunlardan ilki sağlık sektörünün zengin ve değerli veri kaynağına sahip olması, diğeri ise şeffaf (soft) bir hedef olmasıdır [15,18]. Sağlık hizmeti verileri, diğer tüm verilerden çok daha değerlidir. Sağlık örgütlerinde tutulan veriler aynı zamanda politik değere sahiptir [15]. Dünya Anti-Doping Ajansına karşı yapılan saldırılarda önde gelen sporcuların tıbbi kayıtları ifşa edilmesi buna bir örnektir [15,18]. İnsanların sağlık hizmeti sistemlerine dokunmaya cesaret edemeyeceğinden koruyucu önlemlerin gerekli olmadığının düşünülmesi ve sağlık sektörünün hasta bakımı üzerine yoğunlaşması siber güvenliğe yönelik gerekli önlemlerin alınmasına engel olmuştur [15].

Washington Üniversitesi Tıp Fakültesi'nde, kimlik avı yapan bir e-posta, çalışanların e-posta hesaplarına giriş yaparak 80.000'den fazla hastanın sağlık bilgisine erişim sağlamıştır. Washington Üniversitesi Tıp Fakültesi, yaşanan olay sonrası siber güvenlik için yeni bir süreç başlatmalarına rağmen çalınan hasta bilgileri hâlâ güvende değildir [19]. 2016'da, Avustralya Kızıl Haç Kan Bankası donörlerinin risk altındaki cinsel davranışları dahil çok sayıda hassas bilgi içeren 1.28 milyon kayıt, kamuya açık bir web sitesinde yayınlanmıştır [18]. 2016'da 434 yataklı Hollywood Presbiteryen Hastanesinin bilgisayar sistemleri bir hacker tarafından rehin alınmıştır. Sağlık profesyonelleri hastaların tıbbi kayıtlarına erişememiştir ve kağıt üzerinde kayıt tutmak zorunda kalmışlardır. Hollywood Presbyterian Hastanesi'nin, dosyalarına tekrar erişim sağlayabilmesi için 17.000 $'lık ödeme yapması istenmiştir. Yaşanan gelir kaybına ek olarak hastanenin sistemlerine 10 gün boyunca erişim sağlanamamıştır [19,20].

Sağlık hizmetlerinde yaşanan veri ihlalleri, kurumların hizmetlerinin aksamasına, finansal kayıplara sebep olmasının yanı sıra davalar ile karşı karşıya kalınmasına da sebep olmaktadır [21]. Dünya genelin-

de bu konuyla ilgili federal yasalar, veri ihlallerine sebep olan kuruluşlar için ağır cezalar vermektedir. Örneğin Hollywood Presbyterian Hastanesi yanlış yapılandırılmış web sunucuları ve veritabanı erişimi için esnek politikaları nedeniyle 6800 hastanın verilerinin internette açıklanmasıyla 3,3 milyon dolar para cezasına çarptırılmıştır. İlgili bir davada, Columbia Üniversitesi Hollywood Presbyterian Hastanesi veri tabanı sunucularına bağlanmak için kullanılan bilgi teknolojisi ekipmanı üzerinde uygun risk analizlerini yürütmede başarısız olduğu için 1,5 milyon dolarlık para cezası ödemiştir [21].

2011 yılında Joplin'de meydana gelen kasırga sonucu 134 kişi ölmüştür. Joplin'deki bir sağlık kuruluşunda ise yaşanan kasırgada kağıt üzerindeki tüm tıbbi kayıtları kaybedilmiştir. Fırtınadan üç hafta önce, bu kurumda elektronik sağlık kayıtları sistemine geçiş yapılmıştır. Kasırgadan altı gün sonra, sağlık profesyonelleri yeni geçici mobil tıbbi uygulama ile çalışmaya geri dönmüştür. Hasta kayıtlarının tamamına elektronik sağlık kayıtları aracılığıyla ulaşıldığından sağlık profesyonelleri bakım sağlamaya devam edebilmiştir [22].

Siber suçluların hedefi olan sağlık sektöründeki diğer bir tehlike ise hastalar için hayati önem taşıyan akıllı tıbbi cihazlardır [23]. Tıbbi cihazlar giderek veri yönetimi cihazlarına kablosuz olarak bağlanmaktadır [24]. Doğru bilgi ve komut akışına yönelik tehditler, bu cihazların güvenliği; kullanıcıların sağlığı için tehlike oluşturabilir. Bu tür cihazlar ayrıca hastaya iletilmek üzere olan verileri veya komutları içerebilir. Bu cihazlar ayrıca teşhis için (örneğin, manyetik rezonans, bilgisayarlı tomografi, pozitron emisyon tomografi veya ultrason görüntüleme ekipmanı ve yoğun bakım ünite monitörler) veya tedavi için (örneğin, infüzyon pompaları, ventilatörler ve sağlık tesislerinde bulunan tıbbi lazerler) büyük taşınabilir olmayan cihazlar ya da insülin pompası gibi akıllı cihazlar olabilir [23,25]. Amerikan Gıda ve İlaç Dairesi, ritim bozukluğu gibi hastalıkların tedavisinde son yıllarda kullandığı akıllı kalp pillerinin güvenlik zafiyetini öğrenmek için bir dizi test yapmış ve bu cihazların siber korsanlar tarafından ele geçirilebileceğini belirtmiştir. Cihazların güvenliğinin test edildiği araştırmada; kalp piline kablosuz internet üzerinden ulaşılabileceği, korsanların cihazı durdurmakla kalmayıp ölümcül bir elektroşok oluşturabileceği bildirilmiştir. Aynı şekilde; akıllı insülin pompaları siber güvenliğinin hackerlara karşı zayıf olduğu gerekçesiyle piyasadan kaldırılmış ve hastanelerin bu cihazı kullanmasına izin verilmemiştir. Çok fazla sayıda kişinin kullandığı vücutta taşınan insülin pompasının uzaktan kontrol edilerek ilaç dozu miktarının yeniden ayarlanabileceği ve acilde kullanılan ilaç pompalarının uzaktan ele geçirilip bu pompalardan akan sıvıların alt ve üst sınırlarının aşılarak hastaya zarar verilebileceği saptanmıştır [23].

SONUÇ

Siber güvenlik, hastaların güveni, güvenliği ve mahremiyetini korumanın önemli bir parçasıdır. Sağlık teknolojileri ve hasta bilgilerinin güvenliğini sağlamak için daha fazla maliyete ve çabaya ihtiyaç duyulmaktadır. Güvenlik, ürün dizayn edilirken tasarlanmalı sonradan düşünülmemelidir. Siber güvenlik, hasta bakım kültürünün bir parçası haline gelmelidir. Özellikle sağlık sektörü bilişim teknolojilerini kullanmaya başlaması ile politikaların oluşturulmasını zorunlu kılmıştır. Sağlık Sektöründe siber güvenliğin sağlanması için; siber güvenlik teknik yeteneklerinin önceden tanımlanması ve zayıf yönlerinin belirlenmesi, gerekli sağlık işgücü kapasitesinin geliştirilmesi, tıbbi cihazların ve sağlık teknolojisinin güvenliği ve dayanıklılığının artırılması, siber güvenlik konusunda düzenli eğitimlerin gerçekleştirilerek farkındalığın artırılması gerekir.

KAYNAKLAR

1. Yılmaz EN, Ulus Hİ, Gönen S. Bilgi toplumuna geçiş ve siber güvenlik. Bilişim Teknolojileri Dergisi. 2015;8(3):133-46.
https://doi.org/10.17671/btd.87028

2. Özdemirci F. Bilgi-Değişim-Siber Güvenlik-Bağımsızlık. Bilgi Yönetimi. 2018;1(1):78-83.

3. Yayla M. Hukuki bir terim olarak "Siber Savaş". TBB Dergisi. 2013; 177-202.

4. We Are Social Ltd. (2018). Global Digital Report 2018,

URL: https://wearesocial.com/blog/2018/01/global-digital-report-2018 (Erişim Tarihi 09.03.2019).

5. Türkiye İstatistik Kurumu, Girişimlerde Bilişim Teknolojileri Kullanım Araştırması, 2017, Sayı: 24863. URL:http://www.tuik.gov.tr/HbPrint.do?id=24863 (Erişim Tarihi: 09.03.2019).

6. Terzi M. Bilgi ve iletişim teknolojilerine dayalı oluşumlar ile bu oluşumların). Uluslararası ilişkilere güvenlik bağlamındaki etkisi: Siber terörizm 2016-2019 ulusal siber güvenlik strateji belgesi kapsamında Türkiye incelemesi. Kara Harp Okulu Bilim Dergisi. 2018;28(1):73-108.

7. Yılmaz O. Küreselleşme sürecinde dönüşen güvenlik algısı ve siber güvenlik. Cyberpolitik Journal. 2017;2(4):22-43.

8. Hekim H, Başıbüyük O. Siber suçlar ve Türkiye'nin siber güvenlik politikaları. Uluslararası Güvenlik ve Terörizm Dergisi. 2013;4(2):135-8.

9. Önaçan MBK, Atan H. Siber güvenlikte lisansüstü eğitim: Deniz harp okulu örneği. Trakya University Journal of Engineering Sciences. 2016;17(1):13-21.

10. Yeniman Yıldırım E. Bilişim sistemlerine yönelik siber saldırılar ve siber güvenliğin sağlanması. Mesleki Bilimler Dergisi. 2018;7(2):1-11.

11. Aslay F. Siber saldırı yöntemleri ve Türkiye'nin siber güvenlik mevcut durum analizi. International Journal of Multidisciplinary Studies and Innovative Technologies. 2017;1(1):24-8.

12. Çelik S. Siber uzay ve siber güvenliğe multidisipliner bir yaklaşım. Akademic Review of Humanities and Social Sciences. 2017;1(2):110-9.

13. Gökçe KG, Şahinaslan E, Dinçel S. Mobil yaşamda siber güvenlik yaklaşımı. 7. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı; 17-18 Ekim 2014; İstanbul, Türkiye.

14. Öztaş B, Tekin YE, Köse G. Hemşirelik hizmetleri yönetiminde bilişim teknolojilerinin yeri. Türkiye Klinikleri Journal Surgical Nursing-Special Topics. 2016;2(1):5-8.

15. Coventry L, Branley D. Cybersecurity in healthcare: A narrativereview of trends, threats and ways forward. Maturitas. 2018;113:48-52.
https://doi.org/10.1016/j.maturitas.2018.04.008

16. Jalali MS, Kaiser JP. Cybersecurity in hospitals: A systematic, organizational perspective. Journal of Medical Internet Research. 2018;20(5):1-17.
https://doi.org/10.2196/10059

17. Argaw ST, Bempong NE, Eshaya-Chauvin B, Flahault A. Thestate of research on cyber attacks against hospitals and available best practicere commendations: a scopingreview. BMC Medical Informatics and Decision Making. 2019;19(1):1-11.
https://doi.org/10.1186/s12911-018-0724-5

18. Martin G, Martin P, Hankin C, Darzi A, Kinross J. Cybersecurity and healthcare: how safe are we?. British Medical Association. 2017: 1-4.
https://doi.org/10.1136/bmj.j3179

19. Ross J. Cybersecurity: A real threat to patient safety. Journal of Peri Anesthesia Nursing. 2017;32(4):370-2.
https://doi.org/10.1016/j.jopan.2017.05.005

20. Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care. 2017;25(1):1-10.
https://doi.org/10.3233/THC-161263

21. McLeod A, Dolezel D. Cyber-analytics: Modeling factors associated with healthcare data breaches. Decision Support Systems. 2018;108:57-68.
https://doi.org/10.1016/j.dss.2018.02.007

22. Magrabi F, Ong M, Coiera E. Health IT for patient safety and improving the safety of health IT. Studies in Health Teknology and Informatics. 2016;222:25-36.

23. Eke E, Çelik R, Çetin B. Mobil sağlık uygulamalarının güvenliğine ilişkin haberler aracılığıyla yaşanan etik sorunların değerlendirilmesi. AİBÜ Sosyal Bilimler Enstitüsü Dergisi. 2018;18(3):129-45.
https://doi.org/10.11616/asbed.vi.470699

24. Coronado AJ, Wong TL. Healthcare Cybersecurity Risk Management: Keys to an effective plan. Biomedical Instrumentation & Technology: Cybersecurity In Health Care. 2014;48(1):26-30.
https://doi.org/10.2345/0899-8205-48.s1.26

25. Yuan S, Fernando A, Klonoff DC. Standards for medical device cybersecurity in 2018. Journal of Diabetes Science and Technology. 2018;12(4):743-6.
https://doi.org/10.1177/1932296818763634