ULUSLARARASI SAĞLIK YÖNETİMİ VE STRATEJİLERİ ARAŞTIRMA DERGİSİ
INTERNATIONAL JOURNAL OF HEALTH MANAGEMENT AND STRATEGIES RESEARCH
Cilt/Volume : 9 Sayı/Issue : 2 Yıl/Year : 2023 ISSN -2149-6161
Usaysad Derg, 2023; 9(2):269-283 (Derleme makale)

KABLOSUZ AĞA BAĞLI TIBBİ CİHAZLARDA SİBER GÜVENLİK AÇIKLARI VE ÇÖZÜM ÖNERİLERİ

CYBER SECURITY VULNERABILITIES AND SOLUTIONS FOR MEDICAL DEVICES CONNECTED TO WIRELESS NETWORKS

Hüseyin Galip YURTTAŞ
Aselsan, galipyurttas@aselsan.com.tr, orcid.org/0009-0002-2168-474X

Doç. Dr. Alper GÜZEL
Gazi Üniversitesi, guzel@gazi.edu.tr, orcid.org/0000-0003-0492-7500

Makale Gönderim –Kabul Tarihi (25.05.2023-29.08.2023)

Öz

Bu makale, kablosuz ağa bağlı tıbbi cihazlarda siber güvenlik konusunu ele almaktadır. Kablosuz tıbbi cihazların yaygın kullanımı, hastaların sağlık durumlarını izlemek ve tedavi etmek için büyük avantajlar sunmaktadır. Ancak, bu cihazlar, siber saldırılara karşı ciddi riskler taşımaktadır. Bu risklerden faydalanan saldırganların cihazları ele geçirmesi, hasta verilerini elde etmesi veya hastaların sağlığına zarar vermesine sebep olabilmektedir. Araştırmamız, kablosuz tıbbi cihazlarda siber güvenlik zafiyetlerinin çeşitli faktörlerden kaynaklandığını ortaya koymuş, güvenlik zayıflıklarına nasıl önlem alınabileceği konusunda öneriler sunulmuştur. Bu makale, kablosuz tıbbi cihazlardaki güvenlik zayıflıkları ve bu zayıflıkların potansiyel etkilerinin başta bu alanda strateji belirleyici olan regülatörler, kurum yöneticileri olmak üzere cihaz üreticileri ve kullanıcılar tarafından anlaşılması için önemli bir adımdır. Gelecekteki çalışmalarda, bu zayıflıkların giderilmesi ve güvenlik önlemlerinin etkin bir şekilde uygulanması için daha fazla araştırma yapılmasını gerekmektedir. Bu şekilde, kablosuz tıbbi cihazların güvenliği ve hasta güvenliği konusunda önemli bir ilerleme sağlanabilir.

Anahtar Kelimeler: "kablosuz tıbbi cihazlar", "siber güvenlik", "tehditler", "önlemler", "standartlar"

Abstract

This paper addresses the issue of cybersecurity in wireless networked medical devices. The widespread use of wireless medical devices offers great advantages for monitoring and treating patients' health conditions. However, these devices carry serious risks against cyber-attacks. Attackers who exploit these risks can compromise the devices, obtain patient data, or cause harm to patients' health. Our research has revealed that cyber security vulnerabilities in wireless medical devices are caused by various factors, and recommendations are presented on how to take precautions against security weaknesses. This paper is an important step towards understanding the security weaknesses in wireless medical devices and their potential impacts by regulators, institutional managers, device manufacturers and users. In future studies, further

ULUSLARARASI SAĞLIK YÖNETİMİ VE STRATEJİLERİ ARAŞTIRMA DERGİSİ
INTERNATIONAL JOURNAL OF HEALTH MANAGEMENT AND STRATEGIES RESEARCH
Cilt/Volume : 9 Sayı/Issue : 2 Yıl/Year : 2023 ISSN -2149-6161

research is needed to address these weaknesses and to effectively implement security measures. In this way, significant progress can be made in the safety of wireless medical devices and patient safety.

Keywords: wireless medical devices, cyber security, threats, measures, standards

GİRİŞ

Günümüzde, kablosuz ağa bağlı tıbbi cihaz hizmetleri hızla gelişmekte ve kullanımı yaygınlaşmaktadır. Teknolojideki ilerlemeler ve bu gelişmelerin biyomedikal mühendisliği tarafındaki yansımaları ile kablosuz ağa bağlı tıbbi cihazlarının geliştirilmiş ve bu cihazların hasta takip, izleme, teşhis ve kişiye özel tedaviler için kullanımı ve yaygınlaştırılması daha düşük maliyetli ve sürdürülebilir bir sağlık politikası olarak kabul görmüştür (Zhenge vd., 2013). Daha önce tüm hasta bilgileri, sağlık verileri kâğıt üzerine kaydedilir ve arşivlenirdi. Hastaların geçmiş verilerine ulaşmak için arşivlerde birikmiş devasa dosya yığınlarını tek tek incelemek gerekirdi. Teknolojik gelişmeler, dijitalleşme ve özelikle internetin yaygınlaşması iş, seyahat, sağlık ve günlük yaşamı yeniden tanımlamıştır (Tsiatsis vd., 2018). Bu kapsamda tıbbi cihazlar da sağlık hizmetleri alanında büyük bir dönüşüm yaşamaktadır. Özellikle kablosuz teknolojilerin yaygın kullanımı, tıbbi cihazların iletişim kabiliyetini ve hasta izleme yeteneklerini büyük ölçüde artırmıştır. Teknolojik ilerlemeler ve sağlık alanındaki yansımaları, insan sağlığına zarar vermeden biyometrik verilerini toplayabilen kablosuz ağa bağlı tıbbi cihazların gelişimine yol açmıştır (Schumaker, 2020). Bu cihazların kullanımı ve uygulaması, tıp uzmanlarına ve hastalarına vücudun içinde daha önce gizli olan verilere erişim sağlamaktadır (Miraz vd., 2018). Kablosuz tıbbi cihazlar, hastaların sağlık durumunu uzaktan gerçek zamanlı olarak izlemek, hastalara doğru dozda ilaç desteği sağlamak, hasta ile ilgili veri toplamak ve sağlık hizmeti sunucularıyla etkileşimde bulunmak için kullanılan hayati öneme sahip araçlardır. Bu tıbbi cihazlar uzun zamandır giyilebilir ve gömülü sistemler aracılığıyla hastaları kontrol etmek, yönetmek ve izlemek için kullanılmakta olup, bu cihazlar insan hayatını korumada oldukça etkilidir ve tıp uzmanlarının hasta durumu hakkında bilgi sahibi olmalarını ve gelişmiş bakım sağlamalarını mümkün kılmaktadır (Li vd., 2021). Sağlık teknolojilerindeki ve ağa bağlı sensörlerdeki bu ilerlemelerle birlikte sağlık otoriteleri hasta verilerine gerçek zamanlı uzaktan erişim sağladıkları için etkili ve verimli sağlık hizmetleri sunmak için bu cihazları giderek daha yaygın bir şekilde kullanmaktadır. Ağa bağlı tıbbi cihazlar birçok hayat kurtarıcı ve paha biçilmez fayda sağlamaktadır, ancak cihazlar ve veriler güvenli olmayan veri yakalama, veri iletimi, ağ bağlantısı ve birlikte çalışabilirlik ile birlikte gelmektedir (Harit vd., 2017).

Bu ilerlemeler kablosuz tıbbi cihazların siber güvenliği konusu da ciddi bir endişe kaynağı olmuştur. Bu endişeler elektronik ortamda, sağlık kayıtlarının güvenliği, gizlilik ve mahremiyet, veri bütünlüğü ve kullanılabilirliği gibi temel konuları gündeme getirmektedir (Laurinda vd. 2012). Örneğin, Steger (2020) CyberMDX tarafından yayınlanan bir raporda, 120 milyondan fazla taşınabilir kablosuz tıbbi cihazının şu anda hem ev hem de klinik uygulamalarda kullanıldığı ve ihlallere karşı savunmasız olduğu sonucuna varıldığını bildirmiştir. Kimlik verileri, teşhisler, tedavi ve ilerleme notları ve laboratuvar sonuçları gibi klinik bir ortamda paylaşılan veriler gizli kabul edilir ve ülkemizde Kişisel Verileri Koruma Kanunu (KVKK) kapsamında korunmalıdır (KVKK, 2016). Sağlık sektöründe kullanılan kablosuz tıbbi cihazlar giderek daha fazla siber saldırıların hedef haline gelmekte ve siber saldırganlar için cazip bir hedef oluşturmaktadır. Tıbbi cihazların siber saldırılara karşı savunmasız olması hem hastalar hem de sağlık hizmeti sunucuları açısından büyük bir risk oluşturmaktadır. Siber saldırganlar, kablosuz tıbbi cihazlarını hedef alarak cihazlara yetkisiz erişim sağlama, veri manipülasyonu, veri hırsızlığı ve hastaların sağlık durumunu olumsuz etkileme gibi potansiyel zararlı faaliyetlerde bulunabilirler. Kablosuz ağa bağlı tıbbi cihazların

kendine özgü güvenlik açıkları vardır, bu açıklıkların bağlı çevre birimlerindeki siber risk maruziyeti ile birlikte incelenmesi ve toplu bir siber güvenlik çabasının sağlanması hastaların olumsuz etkilenmesini önlemek için gereklidir. (Coventry ve Branley, 2018).

Yaşanan gelişmeler sebebiyle, kablosuz tıbbi cihazlarda siber güvenlik, sağlık sektörünün gündeminde yükselen bir konudur. Ancak Sağlık Hizmetleri Bilgi ve Yönetim Sistemleri Topluluğu (HIMSS) 2020 yılında çok az sayıda sağlık kuruluşunun uçtan uca güvenlik riski değerlendirmesi yaptığını bildirmiştir (HIMSS, 2020). Amerika Birleşik Devletleri Sağlık Hizmetleri Bakanlığı, sağlık hizmeti veren her bir uç noktaya ortalama 816 saldırı girişimi yapıldığını ve bu saldırıların bir önceki yıla göre %9,8 arttığını gösteren bir rapor yayınlamıştır (HHS, 2021). Bu nedenle siber güvenliğe daha bütüncül bakarak, başta politika yapıcılar, kurum yöneticileri, tıbbi cihaz üreticileri ile sağlık personelinde siber güvenlik bilincinin artırılması ve etkili önlemlerin alınması büyük önem taşımaktadır. Kablosuz tıbbi cihazlarda siber güvenlik açıklarının tespit edilmesi, risklerin değerlendirilmesi ve etkili koruma mekanizmalarının geliştirilmesi, hastaların güvenliği, veri bütünlüğü ve veri gizliliği için kritik bir öneme sahiptir.

Bu makale, kablosuz tıbbi cihazlarda siber güvenlik konusunun önemini vurgulamayı ve bu alanda farkındalık oluşturmayı hedeflemektedir. Tıbbi cihazların siber saldırılara karşı savunmasız olması, hastaların güvenliğini ve veri gizliliğini tehlikeye atabilir. Bunlar gibi olumsuz durumların meydana gelmesi hem sağlık hizmeti sunucularının hem de hastaların bu teknolojiye karşı olan güvenini sarsabilir.

Makalede ilk olarak, kablosuz tıbbi cihazların güvenlik açıklarını ve potansiyel tehditleri anlamak için mevcut literatürü gözden geçireceğiz. Kablosuz tıbbi cihazların potansiyel güvenlik açıklarını ve tehditlerini ele alacak ve bunların nasıl sömürülebileceğini açıklayacağız. Bu tehditler arasında yetkisiz erişim, veri manipülasyonu, cihazların devre dışı bırakılması, hatta cihazların ransomware saldırılarına maruz kalması gibi çeşitli senaryolar bulunmaktadır. Bu tehditlerin potansiyel etkilerini ve riskleri değerlendireceğiz. Ardından, bu tehditlere karşı alınabilecek güvenlik önlemlerini ve koruma stratejilerini inceleyeceğiz. Güçlü şifreleme yöntemleri, güçlü kimlik doğrulama, veri şifreleme, ağ güvenliği tedbirleri, düzenli güncellemeler ve güvenlik testleri gibi stratejileri ele alarak, cihazların siber saldırılara karşı nasıl daha dirençli hale getirilebileceğine değineceğiz. Mevcut düzenleyici kurumların hazırlamış olduğu çerçeveleri ve standartları inceleyeceğiz. Düzenleyici kurumların kablosuz tıbbi cihazlarda siber güvenlik konusunda sağladığı rehberlik ve standartlar, tıbbi cihaz üreticileri ve sağlık hizmeti sağlayıcıları için önemli bir kılavuz niteliği taşımaktadır. Bu standartlara uymanın, siber güvenlik açısından önemi vurgulanacaktır. Bu alandaki siber güvenlik önlemlerini uygulamadaki mevcut zorluklar da vurgulanacaktır. Son olarak, sağlık hizmeti sağlayıcıları, cihaz üreticileri ve düzenleyici kurumlar için öneriler sunarak, kablosuz tıbbi cihazlarda siber güvenliğin geliştirilmesine katkıda bulunmayı amaçlamaktayız.

Sonuç olarak, kablosuz tıbbi cihazlarda siber güvenlik, başta cihaz üreticileri, sağlık sektörü çalışanları, olmak üzere hastaların yani herkesin dikkate alması gereken bir konudur. Bu makale, sağlık hizmeti sunucularının, cihaz üreticilerinin, cihaz operatörlerinin, hastaların ve düzenleyici kurumların konuya ilgilisini çekerek kablosuz tıbbi cihazlarda siber güvenlik bilincini artırmayı hedeflemektedir. Bu sayede, hasta ve verilerinin güvenliği sağlanarak, kablosuz tıbbi cihazların potansiyel risklerinin en aza indirilmesine katkıda bulunulabilecektir.

ULUSLARARASI SAĞLIK YÖNETİMİ VE STRATEJİLERİ ARAŞTIRMA DERGİSİ
INTERNATIONAL JOURNAL OF HEALTH MANAGEMENT AND STRATEGIES RESEARCH
Cilt/Volume : 9 Sayı/Issue : 2 Yıl/Year : 2023 ISSN -2149-6161

YÖNTEM

Bu çalışma, bir literatür taraması olarak tasarlanmış ve kablosuz tıbbi cihazlarda siber güvenlik konusunda mevcut araştırmaları sistematik olarak analiz etmek ve güvenlik önlemlerini belirlemek amacıyla gerçekleştirilmiştir.

Veri kaynağı olarak, akademik veri tabanları, bilimsel dergiler, konferans bildirileri, kitaplar ve ilgili endüstri raporları, ilgili kanun ve yönetmelikler gibi çeşitli kaynaklar kullanılmıştır. IEEE Xplore, PubMed, Scopus ve Web of Science gibi önemli veri tabanları taranmış ve güncel araştırmalar elde edilmiştir.

Veri toplama süreci, belirlenen anahtar kelimeler ve filtreleme kriterleri kullanılarak gerçekleştirilmiştir. İlgili çalışmaları içeren makaleler ve diğer kaynaklar tarama süreciyle toplanmıştır. Elde edilen makaleler ve diğer veriler, daha sonra ayrıntılı bir şekilde incelenmiş ve analiz edilmiştir. Toplanan veriler, nitel ve nicel yöntemler kullanılarak analiz edilmiştir. Nitel veriler, içerik analizi yöntemiyle temalar ve kavramlar üzerinde yapılandırılmış bir analizle incelenmiştir. Nicel veriler ise istatistiksel analizler kullanılarak, eğilimler, oranlar ve ilişkiler üzerinde bir değerlendirme yapılmıştır.

Etik Düşünceler

Bu literatür taraması çalışması, mevcut araştırmaların analizini içermekte olup, katılımcılarla ilgili veri toplama aşaması içermemektedir. Etik konular, literatürdeki çalışmaların etik standartlara uygun olup olmadığını değerlendirmek amacıyla gözden geçirilmiştir.

Sınırlamalar:

Bu çalışmanın bazı sınırlamaları bulunmaktadır. Bunlar arasında ingilizce kaynakların daha yoğun kullanılması, belirli bir zaman aralığını kapsaması ve belirli veri tabanlarına odaklanması sayılabilir. Ülkemizin özellikle tıbbi alanda gelişen teknolojiden çok uzak olmadığı düşünüldüğünde elde edilen sonuçların genel olarak geçerli olacağı düşünülebilir ancak sayılan sınırlamaların elde edilen sonuçların genel geçerliliğini etkileyebileceği göz önünde bulundurulmalıdır.

BULGULAR

Literatür taraması sonucunda, kablosuz ağa bağlı tıbbi cihazların kullanım alanlarının oldukça genişlediği görülmüştür. Kablosuz ağa bağlı tıbbi cihazların gelişimi nesnelerin interneti alanındaki ilerlemeler ile birlikte başlamış ve dijital sağlık alanında ve hastaların önemli yaşamsal değerlerinin izlenmesi ile hasta bakımı konularında farklı bir çözüm sunmuştur. (Sun vd., 2018). Bunlar arasında adımsayar, kalp atış hızı, kandaki oksijen miktarı, hareket algılayabilen, sıcaklık ölçen, glikoz seviyesi takibi yapabilen, fitness takibi yapabilen ve kilo ölçümü yapabilen cihazlar giyilebilir tıbbi cihazlar olarak sayılabilir (Schumaker, 2020). İlgili tıbbi cihazlara kalp pilleri, defibrilatörler, aritmi dedektörleri, kronik ağrıları, depresyon etkilerini veya zihinsel bozuklukları konusunda etkili olabilen beyin implantları ve ameliyatla vücut içine yerleştirilmiş gömülü veya implante edilmiş hasta yaşam kalitesini etkileyen cihazlar örnek gösterilebilir (McFarland & Olatunbosun, 2019). Bahsi geçen tüm bu kablosuz tıbbi cihazlarda çeşitli güvenlik açıklıklarının mevcut olduğu tespit edilmiştir. İlgili güvenlik açıkları; kablosuz tıbbi cihazlarındaki, etkileşimde bulunduğu ağdaki, donanımdaki, veri toplama sürecindeki, veri aktarımlarındaki ve siber güvenlik uygulamalarındaki güvenlik mekanizmalarının eksikliğinden kaynaklanmaktadır (Maras, 2015). Maalesef, bilgi teknolojileri alanındaki kanun koyucular ve sorumlu yöneticiler, ağı ve verileri

korumak için gerekli güvenlik uygulamalarını devreye almış, ancak tıbbi cihazları istemsizce bu koruma çemberine dahil etmemiştir (Morgan, 2019). Bu nedenle korunmasız kablosuz tıbbi cihazlar bir yandan insan sağlığının korunması dolayısıyla insanlık için çok önemli fırsatlar sunarken diğer yandan ciddi güvenlik sorunlarına da sebep olmaktadır (Omolara vd., 2021). Güvenlik açıkları, şifresiz veri aktarımları, radyo frekansı iletimleri, sabit kodlanmış yönetici şifreleri, kimlik doğrulama eksikliği, yanlış ağ yapılandırmaları ve yazılım kütüphanesi güvenlik açıkları (Deloitte, 2013; Garcia, 2017) olarak sıralanabilir. Ağa bağlı tıbbi cihazların güvenlik açıklarına örnek olarak Microsoft'un Uzak Masaüstü Protokol Hizmeti ve bağlı tıbbi cihazlarla ilgili sorun verilebilir (HIPAA Ransomware, 2017). Sadece İskoçya ve İrlanda'da on bin Siemens ve Bayer ağa bağlı tıbbi cihazı ve 200.000'den fazla mağdur etkilenmiştir. Saldırı uluslararası sınırları aşmış ve Amerika Birleşik Devletleri'ndeki Bayer MedRad cihazlarını etkilemiştir. Araştırmamız, bu zayıflıkların ciddi riskler taşıdığını ve siber saldırılara açık bir hedef oluşturduğunu ortaya koymuştur (Thielfoldt, 2022). Aşağıda bu güvenlik açıklıklardan bazıları daha detaylı belirtilmiştir.

Zayıf Şifreleme Yöntemleri: Kablosuz tıbbi cihazlarda kullanılan şifreleme yöntemleri, çoğu zaman yeterli düzeyde olmamaktadır. Zayıf veya kırılması kolay şifreleme algoritmaları kullanıldığında, saldırganlar cihaza yetkisiz erişim sağlayabilir ve hastaların verilerine müdahale edebilir.

Yetkilendirme ve Kimlik Doğrulama Eksiklikleri: Kablosuz tıbbi cihazlar, hastaların sağlık verilerini korumak için doğru yetkilendirme ve kimlik doğrulama süreçlerine ihtiyaç duyar. Ancak, bazı cihazlarda bu süreçlerin yetersiz olduğu görülmüştür. Zayıf veya hatalı yetkilendirme mekanizmaları, saldırganların cihaza yetkisiz erişim sağlamasına ve veri manipülasyonuna yol açabilir.

Yazılım Güncelleme Süreçlerindeki Aksaklıklar: Kablosuz tıbbi cihazların yazılım güncellemeleri, güvenlik açıklarının kapatılması ve yeni güvenlik önlemlerinin uygulanması için kritik öneme sahiptir. Ancak, bazı cihazlarda güncelleme süreçlerinde aksaklıklar görülmüştür. Bu durum, güncellemelerin zamanında yapılmamasına ve güvenlik açıklarının kapatılmamasına yol açarak saldırganların cihaza sızmasına olanak tanır.

Ağ Trafiğindeki Güvenlik Açıkları: Kablosuz tıbbi cihazlar, hastaların verilerini iletmek için bir ağa bağlanır. Ancak, ağ trafiği üzerindeki güvenlik açıkları, saldırganların verileri izlemesine, manipüle etmesine veya çalmalarına olanak tanır. Bu konuda HP firması, cihazlarda donanım bazlı güvenlik eksikliğine gelmeden, yerel ve genel internet ağlarının güvenli bir iletişim ortamı sunmadığı sonucuna varmıştır (Kovacs, 2014). Zayıf ağ güvenliği önlemleri ve korumasız iletişim kanalları, bu tür saldırılara karşı cihazları savunmasız hale getirir.

İlgili Yetkililerin ve Personelin Siber Güvenlik konusundaki Eğitimsizliği: Kablosuz tıbbi cihazların güvenliği, sadece teknik önlemlerle sınırlı değildir. İlgili sağlık personelinin siber güvenlik konusunda yeterli eğitim almamış olması, cihazların güvenli kullanımını etkileyen bir zayıflıktır. Eğitimsiz personel, cihazların güvenlik özelliklerini ve doğru kullanım yöntemlerini bilmeyebilir, güvenlik protokollerini takip etmeyebilir veya saldırıların belirtilerini tanıyamayabilir. Sağlık alanında çalışan uzmanlar kablosuz tıbbi cihazların hasta hayatını ve bakımını kolaylaştırma potansiyelinin farkındadır, ancak bu alandaki siber güvenlik farkındalığı konusunda önemli eksiklikler bulunmaktadır (Martin vd., 2017). Tıbbi cihaz üreticileri, cihazlarla birlikte gelen siber güvenlik açıklıkları üzerine bir kavrayış geliştirmeden ilgili aletlerin imalatında aceleci davranmıştır. Alsubaei ve diğerleri (2019) cihaz satıcılarının kablosuz tıbbi cihazlardaki siber güvenlik açıklıkları konusundaki farkındalık oranının %17 olduğunu belirtmiştir. Bu da cihazların

siber saldırılara daha açık hale gelmesine ve hastaların güvenliğini tehlikeye atmasına önemli bir neden olabilir.

Bu bulgular, kablosuz tıbbi cihazlarda siber güvenlik zayıflıklarının varlığını ve ciddi riskler taşıdığını vurgulamaktadır. Bu zayıflıkların giderilmesi ve güvenlik önlemlerinin iyileştirilmesi için sağlık sektöründe daha fazla çalışma ve yatırım yapılması gerekmektedir. Bu şekilde, kablosuz tıbbi cihazların güvenliği artırılabilir ve hastaların sağlık bilgileri daha iyi korunabilir.

Endüstri Standartları ve Yönetmelikler

Kablosuz tıbbi cihazlarda siber güvenlikle ilgili olarak, endüstri standartları ve yönetmelikler incelenmiştir.

ISO 27001: Kablosuz tıbbi cihazlarla ilgili siber güvenlik yönetim sistemi için en yaygın kullanılan standartlardan biri ISO 27001'dir. Bu standart, güvenlik risklerinin etkili bir şekilde yönetilmesini sağlayan bir çerçeve sunar. ISO 27001, güvenlik politikaları, risk değerlendirmesi, güvenlik kontrolleri, sürekli iyileştirme ve sürdürülebilirlik gibi konuları kapsar.

IEC 62304: Tıbbi cihazların yazılımının yaşam döngüsü sürecini kapsayan IEC 62304 standardı, kablosuz tıbbi cihazların güvenli yazılım geliştirme sürecini düzenler. Bu standart, yazılım gereksinimleri, tasarım, test, doğrulama ve doğruluk doğrulama gibi aşamaları içerir ve cihazın güvenli ve etkili çalışmasını sağlamak için önemli bir rol oynar.

FDA Yönetmelikleri: Amerika Birleşik Devletleri'nde kablosuz tıbbi cihazların pazarlanması ve kullanımıyla ilgili FDA (Food and Drug Administration) yönetmelikleri önemlidir. FDA, tıbbi cihazların güvenliği, performansı ve etkinliği konularında yönergeler ve gereklilikler sunar. Kablosuz tıbbi cihazlar için FDA tarafından belirlenen özel gereklilikler ve siber güvenlik konusunda yönergeler vardır.

UL 2900: UL (Underwriters Laboratories) tarafından geliştirilen UL 2900 standardı, tıbbi cihazların siber güvenliği için bir çerçeve sunar. Bu standardın amacı, cihazların güvenliğini ve siber tehditlere karşı direncini değerlendirmek ve sertifikalandırmaktır. UL 2900, tıbbi cihazların siber güvenlik testlerini ve değerlendirmelerini yönlendiren bir referans haline gelmiştir.

Avrupa Birliği Tıbbi Cihaz Yönetmeliği (MDR): Avrupa Birliği'nde kablosuz tıbbi cihazların pazarlanması ve kullanımıyla ilgili MDR (Medical Device Regulation) yönetmeliği geçerlidir. MDR, tıbbi cihazların güvenliği, performansı, kalite ve uyumluluk gerekliliklerini belirler. Bu yönetmelik, kablosuz tıbbi cihazlar için de özel gereklilikler ve siber güvenlik konusunda yönergeler içerir.

Ülkemizde KVKK ile genel olarak hukuki koruma altına alınmasına ek olarak Türkiye Cumhuriyeti Sağlık Bakanlığı 2019 yılında “Tıbbi Cihazlarda Alınması Gereken Güvenlik Önlemleri Dokümanı” yayınlayarak bu cihazların siber güvenlik önlemleri ile kullanımı için rehberlik sağlamaktadır.

Endüstri standartları ve yönetmelikler, kablosuz tıbbi cihazların güvenliği için belirli gereklilikler ve kılavuzlar sağlar. Bu standartları ve yönetmelikleri takip etmek, cihazların güvenliği ve uyumluluğu açısından önemlidir ve tıbbi cihaz üreticileri, sağlık kuruluşları ve düzenleyici otoriteler tarafından dikkate alınması gereken bir konudur.

ULUSLARARASI SAĞLIK YÖNETİMİ VE STRATEJİLERİ ARAŞTIRMA DERGİSİ
INTERNATIONAL JOURNAL OF HEALTH MANAGEMENT AND STRATEGIES RESEARCH
Cilt/Volume : 9 Sayı/Issue : 2 Yıl/Year : 2023 ISSN -2149-6161

Tehdit Modelleri ve Saldırı Senaryoları

Kablosuz tıbbi cihazlar için tehdit modelleri ve saldırı senaryoları incelenmiştir. Araştırmalar, kötü niyetli saldırganların cihazları ele geçirerek hastalara zarar verebilecek veya hassas sağlık verilerine erişebileceğini göstermektedir. Saldırı senaryoları arasında veri manipülasyonu, kimlik hırsızlığı ve hizmet kesintisi gibi durumlar yer almaktadır.

DoS (Hizmet Engelleme) Saldırıları: Saldırganlar, kablosuz tıbbi cihazlara sürekli istekler göndererek kaynakları tüketebilir ve cihazın normal işleyişini engelleyebilir. Bu tür bir saldırı, hastaların tedavisini etkileyebilir veya tıbbi cihazın işlevselliğini engelleyebilir.

Veri Manipülasyonu: Saldırganlar, kablosuz tıbbi cihazlara erişerek hastaların sağlık verilerini manipüle edebilir. Bu durum hatalı teşhis ve yanlış tedavilerin yapılmasına sebebiyet verebilir. Sağlık alanında veri ihlalleri son beş yılda %300 oranında artmış olduğu görülmüş ve ilgili hizmet sağlayıcı kurumların çoğunun siber güvenlik savunmalarına güvenmediği anlaşılmıştır (Martin vd., 2017).

Kimlik Hırsızlığı: Saldırganlar, kablosuz tıbbi cihazlardaki güvenlik zayıflıklarından yararlanarak hasta kimliklerini çalabilir. Bu durum, sahte tedavi talepleriyle mali kayıplara veya hastaların yanlış tedavi almasına yol açabilir.

İzleme ve Casusluk: Saldırganlar, kablosuz tıbbi cihazlara yetkisiz erişim sağlayarak hastaların sağlık verilerini izleyebilir ve gizli bilgileri ele geçirebilir. Bu durum, hastaların mahremiyetinin ihlal edilmesine ve kişisel bilgilerin kötüye kullanılmasına neden olabilir.

Uzaktan Kontrol: Saldırganlar, kablosuz tıbbi cihazlara sızarak cihazın kontrolünü ele geçirebilir ve hasta tedavisini etkileyebilir. Bu tür bir saldırı, cihazın yanlış bir şekilde çalışmasına veya hastaların gerektiği gibi tedavi edilmemesine yol açabilir.

Fiziksel Tehditler: Kablosuz tıbbi cihazlar, fiziksel olarak güvende olmadıklarında da risk altındadır. Saldırganlar, cihazları fiziksel olarak ele geçirerek veya zarar vererek hastaların sağlığını tehlikeye atabilir.

Ransomware saldırıları: Kablosuz tıbbi cihazlar, fidye yazılımları tarafından hedef alınabilir ve kullanılamaz hale getirilebilir.

Bu tehdit modelleri ve saldırı senaryoları, kablosuz tıbbi cihazların karşı karşıya olduğu güvenlik risklerini vurgulamaktadır. Bu risklerin dikkate alınması ve gerekli güvenlik önlemlerinin alınması, hastaların güvenliği ve tıbbi cihazların güvenliği açısından önemlidir.

Mevcut Güvenlik Önlemleri

Literatürde, kablosuz tıbbi cihazlarda siber güvenliği artırmak için kullanılan mevcut güvenlik önlemleri incelenmiştir. Kablosuz tıbbi cihazlarda siber güvenliği sağlamak için çok disiplinli bir yaklaşım benimsemek önemlidir. İlgili cihazlar ve bağlı olduğu tüm ortamlar için top siber güvenlik önlemleri alınmalıdır. Sağlık hizmeti sunucuları, cihaz üreticileri, siber güvenlik uzmanları ve düzenleyici kurumlar arasında iş birliği yapılmalıdır. Risk değerlendirmeleri yapılmalı, güvenlik açıklarının tespiti ve düzeltilmesi için sürekli izleme yapılmalıdır. İlgili çalışanlara düzenli olarak konuyla ilgili eğitimler verilmeli ve aralıklarla farkındalık arttırıcı uygulamalar devreye alınmalıdır. Bununla beraber uygulanabilecek diğer güvenlik önlemleri şu şekilde sayılabilir.

İlgili Standartlara ve Yönetmeliklere Uyum: Düzenleyici kurumlar, kablosuz tıbbi cihazlarda siber güvenlik standartları ve gereksinimleri belirlemişlerdir Kablosuz tıbbi cihazların güvenliği için

geçerli standartlara ve yönetmeliklere uyum sağlanmalıdır. Ancak her zaman güncel kalmak ve ilgili düzenlemeleri ve en iyi uygulamaları düzenli olarak takip etmek önemlidir. Teknoloji hızla ilerlemekte ve siber saldırganların yöntemleri de değişmektedir, bu nedenle güvenlik tedbirleri standartlarının da buna paralel olarak sürekli olarak güncellenmesi gerekmektedir.

Veri şifrelemesi, Kablosuz tıbbi cihazlardan iletilen verilerin şifrelenmesi, veri güvenliğini sağlamak için önemlidir. Bu, hassas sağlık verilerinin korunmasına yardımcı olur ve veri hırsızlığı riskini azaltır.

Güvenlik testleri, cihazların potansiyel zayıf noktalarını tespit etmek ve düzeltme süreçlerini yönlendirmek için yapılmalıdır.

Güçlü Şifreleme Algoritmaları: Kablosuz tıbbi cihazlar için güçlü şifreleme algoritmalarının kullanılması, verilerin korunmasında önemli bir rol oynar. Güçlü ve kırılması zor şifreleme algoritmaları, yetkisiz erişimi zorlaştırarak hastaların sağlık verilerinin gizliliğini sağlar.

Yetkilendirme ve Kimlik Doğrulama: İlgili personel ve cihazların doğru bir şekilde yetkilendirilmesi ve kimlik doğrulama süreçlerinin uygulanması önemlidir. Kullanıcıların doğru kimlik bilgileriyle cihaza erişmeleri ve yetkilendirme süreçlerini tamamlamaları, yetkisiz erişimi engeller. Bunun için çözüm olarak sunulan harici donanımlar çoğunlukla tıbbi cihazın çalışması sırasında cihaza yetkilendirme ve kimlik doğrulama süreçlerini uygulamaya koyarak erişim kontrolünü artırmayı amaçlarken acil durumlarda cihaza hızlı erişimin önündeki engelleri de kaldırmayı sağlayabilmektedir. Örneğin güvenlik seviyesini yükseltmek için Cloaker (Denning vd., 2008), IMD Guard (Xu vd., 2011) ve IMD Shield (Gollakota vd., 2011) gibi bazı harici donanım kullanma gibi önerilerde bulunulmuştur.

Güvenli Yazılım Güncelleme Süreci: Kablosuz tıbbi cihazların yazılımlarının güncel tutulması, güvenlik açıklarının kapatılması için kritik öneme sahiptir. Buna örnek olarak tıbbi cihazlara yapılan siber saldırılarda kullanılan güvenlik açıklıklarına eski versiyon işletim sistemlerinin sebep olduğunu belirten kötü amaçlı yazılım analiz raporu, MEDJACK 2 tarafından yayınlamıştır (TrapX Research Labs, 2021). Üreticilerin düzenli olarak güvenlik güncellemeleri yayınlaması ve hastaneler veya sağlık kuruluşları tarafından bu güncellemelerin zamanında uygulanması gerekmektedir.

Ağ Güvenliği: Kablosuz tıbbi cihazlar ağlara bağlandığından, ağ güvenliği önlemleri alınmalıdır. Güvenlik duvarları, ağ segmentasyonu, ağ izleme ve saldırı tespit sistemleri gibi önlemlerle ağ trafiği ve iletişim kanalları güvence altına alınabilir. ağ izleme ve saldırı tespit sistemleri ağ trafiği üzerinden uygulama ve ağ performansı hakkında bilgi toplar. Bu sayede performans kaybı olaylarında bilgilendirme yapabilir ve sorunun kaynağı ile alakalı ilgili personele detaylı bilgiyi sağlar.

Fiziksel Güvenlik: Kablosuz tıbbi cihazların fiziksel olarak güvende olması da önemlidir. Cihazların güvenli bir şekilde saklanması, yetkisiz fiziksel erişimi engeller ve cihazların manipülasyon veya zarar görmesini önler.

Saldırı Tespit Sistemleri: Saldırı tespit sistemleri, kablosuz tıbbi cihazlara yönelik olası saldırıları izler ve anormal aktiviteleri tespit eder. Bu sistemler, saldırılara hızlı bir şekilde tepki verilmesini ve müdahale edilmesini sağlar.

Kullanıcı Farkındalığı ve Eğitim

Bulgular, kullanıcıların kablosuz tıbbi cihazların güvenlik risklerine karşı farkındalığının önemini vurgulamaktadır. Bu nedenle farkındalık ve eğitim başlığı biraz daha detaylı hazırlanmıştır. Eğitim

ULUSLARARASI SAĞLIK YÖNETİMİ VE STRATEJİLERİ ARAŞTIRMA DERGİSİ
INTERNATIONAL JOURNAL OF HEALTH MANAGEMENT AND STRATEGIES RESEARCH
Cilt/Volume : 9 Sayı/Issue : 2 Yıl/Year : 2023 ISSN -2149-6161

programları ve bilgilendirme faaliyetleri aracılığıyla, tıbbi personel ve hastaların güvenlik konusunda bilinçli olmaları ve doğru önlemleri almaları sağlanabilir.

Kullanıcı Farkındalığı; kablosuz tıbbi cihazların güvenliği konusunda oldukça önemlidir. Kullanıcılar, cihazların potansiyel risklerini ve güvenlik önlemlerini anlamalı, cihazların güvenli kullanımı konusunda bilinçlenmelidir. Kullanıcı farkındalığı, güvenlik açıklarının fark edilmesi, riskli durumların raporlanması ve uygun önlemlerin alınması açısından kritik bir rol oynar.

Eğitim Programları: Kullanıcıların kablosuz tıbbi cihazlarla ilgili güvenlik konularında eğitilmesi, güvenli kullanımın sağlanması için önemlidir. Eğitim programları, kullanıcılara cihazların güvenli kullanımıyla ilgili bilgi verir, güvenlik protokolleri ve önlemler hakkında farkındalık yaratır. Bu programlar, cihazların nasıl korunacağı, kimlik doğrulama yöntemleri, güvenli veri paylaşımı gibi konuları kapsayabilir. Ayrıca, güncel tehditler ve saldırı senaryoları hakkında da bilgilendirme yapılabilir.

Kullanıcı Sorumlulukları: Kullanıcıların kablosuz tıbbi cihazların güvenliği için belirli sorumlulukları vardır. Eğitim programları, kullanıcıların bu sorumlulukları anlamasını sağlar. Kullanıcılar, cihazlarını güncel tutmak, yazılım güncellemelerini zamanında uygulamak, güvenlik ayarlarını doğru şekilde yapılandırmak, kimlik doğrulama ve parola yönetimine dikkat etmek gibi önemli adımları takip etmelidir.

Uygulama ve İzleme: Kullanıcı farkındalığı ve eğitim programları, uygulama ve izleme süreçleriyle desteklenmelidir. Kullanıcıların güvenlik politikalarına uyması ve güvenlik önlemlerini doğru şekilde uygulaması için sürekli olarak takip edilmelidir. Kullanıcıların güvenlik ihlallerini veya potansiyel riskleri raporlama mekanizmaları da sağlanmalıdır.

Kullanıcı farkındalığı ve eğitim, kablosuz tıbbi cihazların güvenliği açısından kritik bir faktördür. Kullanıcıların güvenlik konularında bilinçlenmesi, cihazların güvenli kullanımı ve potansiyel risklerin en aza indirilmesi açısından önemlidir. Bu nedenle, kullanıcı farkındalığını artırmaya yönelik eğitim programları düzenlenmeli ve kullanıcıların sorumlulukları vurgulanmalıdır.

Tüm bu önerilerin uygulanabilirliği kurum bünyesinde bulunan cihazların teknolojik yeterlilikleri ile kısıtlı kalacaktır. Bu gibi güncel standartlara uygun protokolleri, şifreleme standartlarını sağlayamayan kritik açıklıkları olan cihazlar varsa bu cihazların ağa bağlı çalışmaması güvenlik açısından en doğrusu olabilir.

Bu mevcut güvenlik önlemleri, kablosuz tıbbi cihazların güvenliğini artırmak için uygulanabilir. Bunlar, üretici firmalar, sağlık kuruluşları ve ilgili personel arasında iş birliğiyle gerçekleştirilmesi gerekmektedir.

Risk Değerlendirmesi

İlgili kurumlar tarafından kablosuz tıbbi cihazların güvenlik zayıflıklarının ve potansiyel saldırı senaryolarının bir risk değerlendirmesi yapılmalıdır. Bu risk değerlendirmesi, cihazların ve hastaların maruz kaldığı potansiyel riskleri ve olası etkilerini belirlemek amacıyla aşağıda belirtilen adımlar kullanılarak gerçekleştirilebilir.

Tehdit Analizi: Kablosuz tıbbi cihazların güvenlik risklerinin değerlendirilmesi için öncelikle potansiyel tehditlerin analizi yapılır. Bu aşamada, cihazların hedef alınabileceği saldırılar ve tehdit senaryoları belirlenir. Örneğin, cihazın kötü niyetli bir kişi tarafından ele geçirilmesi veya ağ üzerinden saldırıya maruz kalması gibi senaryolar göz önünde bulundurulur.

Zayıflık Değerlendirmesi: Kablosuz tıbbi cihazların zayıflıkları ve güvenlik açıkları tespit edilir. Bu aşamada, cihazların yazılım ve donanım bileşenleri, iletişim protokolleri, kimlik doğrulama süreçleri ve diğer güvenlik önlemleri incelenir. Zayıflıkların belirlenmesi, potansiyel risklerin ortaya çıkarılması açısından önemlidir.

Risk Olasılığının ve Etkisinin Değerlendirilmesi: Kablosuz tıbbi cihazların güvenlik riskleri, gerçekleşme olasılıkları ve etkileri açısından değerlendirilir. Riskin olasılığı, tehditlerin gerçekleşme ihtimaline, etki ise gerçekleştiğinde ortaya çıkabilecek zararın derecesine bağlı olarak belirlenir. Bu değerlendirme, riskleri önceliklendirme ve kaynakların doğru şekilde tahsis edilmesi için önemlidir.

Risk Yönetimi Stratejileri: Kablosuz tıbbi cihazların güvenlik risklerini yönetmek için çeşitli stratejiler uygulanır. Bu stratejiler arasında riskin kabul edilmesi, riskin azaltılması için önlemler alınması, riskin transfer edilmesi veya riskin tamamen önlenmesi yer alabilir. Risk yönetimi stratejileri, güvenlik önlemlerinin belirlenmesi ve uygulanması sürecinde rehberlik sağlar.

Sürekli İyileştirme: Risk değerlendirmesi süreci bir süreklilik arz eder. Kablosuz tıbbi cihazların güvenlik riskleri sürekli olarak gözden geçirilir ve değerlendirilir. Yeni tehditler ve zayıflıklar ortaya çıktıkça, risk değerlendirmesi güncellenir ve uygun güvenlik önlemleri alınır. Bu şekilde, kablosuz tıbbi cihazların güvenliği sürekli olarak iyileştirilir.

Risk değerlendirmesi, kablosuz tıbbi cihazların güvenliğini sağlamak için önemli bir adımdır. Bu süreç, potansiyel risklerin belirlenmesi, değerlendirilmesi ve yönetilmesi yoluyla güvenlik önlemlerinin etkin bir şekilde uygulanmasını sağlar.

Gelecek Çalışmalar İçin Yön Verme

Son olarak, bu çalışmanın bulguları temel alınarak gelecekte yapılacak araştırmalar için yönlendirmeler yapılabilir. Örneğin, kablosuz tıbbi cihazlarda yapılacak daha kapsamlı güvenlik testleri, yeni güvenlik mekanizmalarının geliştirilmesi veya kullanıcı deneyimine odaklanan araştırmalar gibi konular gelecek çalışmalara ilham verebilir.

Güvenlik Duvarları: Kablosuz tıbbi cihazlarda güvenlik duvarlarının etkinliği ve performansı daha fazla araştırılmalıdır. Bu, güvenlik duvarlarının potansiyel saldırılara karşı ne kadar etkili olduğunu ve daha iyi koruma sağlamak için nasıl geliştirilebileceğini anlamamıza yardımcı olacaktır.

İleri Şifreleme Teknolojileri: Kablosuz tıbbi cihazlarda kullanılan şifreleme teknolojileri üzerine daha fazla çalışma yapılmalıdır. Gelişmiş şifreleme yöntemleri ve algoritmaları, güvenliği daha da güçlendirmek için araştırılmalıdır.

Saldırı Tespit ve Önleme: Kablosuz tıbbi cihazların saldırılara karşı daha etkili bir şekilde tespit edilmesi ve önlenmesi için çalışmalar yapılmalıdır. Yapay zekâ ve makine öğrenme gibi teknolojiler, anormal aktiviteleri tespit etmek ve potansiyel saldırıları önlemek için kullanılabilir.

Eğitim ve Farkındalık: Kullanıcıların ve sağlık personelinin kablosuz tıbbi cihazların güvenliği konusunda daha fazla eğitim alması ve farkındalığının artırılması önemlidir. Eğitim programlarının etkinliği ve kullanıcı davranışları üzerindeki etkisi üzerine çalışmalar yapılmalıdır.

Yeni Nesil İletişim Protokolleri: Kablosuz iletişim protokollerinin güvenliği için daha güçlü ve güvenli protokollerin geliştirilmesi önemlidir. Bu, veri bütünlüğünü, gizliliğini ve doğruluğunu sağlamak için iletişim kanallarının daha iyi korunmasına katkı sağlayacaktır.

ULUSLARARASI SAĞLIK YÖNETİMİ VE STRATEJİLERİ ARAŞTIRMA DERGİSİ
INTERNATIONAL JOURNAL OF HEALTH MANAGEMENT AND STRATEGIES RESEARCH
Cilt/Volume : 9 Sayı/Issue : 2 Yıl/Year : 2023 ISSN -2149-6161

Zayıf Nokta Analizi: Kablosuz tıbbi cihazların zayıf noktalarının daha iyi anlaşılması için zayıf nokta analizi yapılmalıdır. Bu, cihazların güvenlik açıklarının tespit edilmesini sağlar ve bu açıkların kapatılması için yönlendirmeler sunar.

İş birliği ve Paylaşım: Tıbbi cihaz üreticileri, sağlık kuruluşları, araştırmacılar ve düzenleyici otoriteler arasında daha fazla işbirliği ve bilgi paylaşımı yapılmalıdır. Bu, sektördeki güvenlik standartlarının geliştirilmesini, en iyi uygulamaların yaygınlaştırılmasını ve siber güvenlik risklerinin ortak bir şekilde ele alınmasını sağlar.

Bu yönlendirmeler, kablosuz tıbbi cihazların siber güvenliğiyle ilgili gelecek çalışmalar için rehberlik sağlar. Bu alanlarda yapılan araştırmalar, kablosuz tıbbi cihazların güvenliğini iyileştirmeye ve potansiyel riskleri azaltmaya yardımcı olacaktır.

TARTIŞMA

Bu çalışmanın bulguları, kablosuz tıbbi cihazlardaki güvenlik zayıflıklarının aşağıdaki gibi bazı ciddi potansiyel etkilere sahip olabileceğini göstermektedir.

Hastaların Güvenliği Tehdidi: Kablosuz tıbbi cihazların güvenlik zayıflıkları, hastaların sağlığını doğrudan etkileyebilir. Örneğin, bir saldırganın bir tıbbi cihaza yetkisiz erişim sağlaması veya cihazı manipüle etmesi, hastaların tedavi sürecini bozabilir veya yanlış sonuçlara yol açabilir. Bu durum, hastaların sağlık durumunu olumsuz etkileyebilir ve hatta yaşamlarını riske atabilir.

Gizlilik İhlali: Güvenlik zayıflıkları, kablosuz tıbbi cihazlardan iletilen hassas sağlık verilerinin gizliliğini tehlikeye atabilir. Bir saldırganın veri hırsızlığı yapması veya izinsiz erişim sağlaması durumunda, hastaların kişisel ve tıbbi bilgileri ifşa olabilir. Bu durum, hastaların mahremiyetini ve gizliliğini ihlal eder ve potansiyel olarak sosyal, hukuki veya ekonomik sorunlara yol açabilir.

Sağlık Hizmetlerinin Sürekliliği: Güvenlik zayıflıkları, kablosuz tıbbi cihazların işlevselliğini etkileyebilir ve sağlık hizmetlerinin sürekliliğini tehlikeye atabilir. Bir saldırı veya cihazın yanlış yapılandırılması durumunda, cihazların düzgün çalışması engellenebilir veya kesintiye uğrayabilir. Bu da hastaların tedavi sürecini aksatabilir, sağlık profesyonellerinin doğru kararlar almasını zorlaştırabilir ve acil durumlarda potansiyel riskler yaratabilir.

Güven Kaybı ve İtibar Zararı: Güvenlik zayıflıkları ve siber saldırılar, tıbbi cihaz üreticilerinin ve sağlık kuruluşlarının itibarını zedeler. Hastalar, sağlık hizmeti sağlayıcıları ve endüstri paydaşları, güvenli ve güvenilir bir şekilde çalışan kablosuz tıbbi cihazlara olan güvenlerini kaybedebilir. Bu durum, sektörün genelinde güveni sarstığı gibi, yeni teknolojilerin kabulünü ve benimsenmesini de olumsuz etkileyebilir.

İncelenen güvenlik önlemleri, kablosuz tıbbi cihazlarda siber güvenliği artırmak için alınan adımları yansıtmaktadır. Ancak, tartışmaya açık olan noktalar da vardır. Örneğin, mevcut güvenlik önlemlerinin kullanılabilirliği ve etkinliği konusunda bazı sınırlamalar olabilir. Bunun yanı sıra, güvenlik önlemlerinin uygulanması ve yönetimi konusunda karşılaşılan zorluklar da değerlendirilmelidir. Siber güvenlik sağlanması için tasarlanan çözümlerde ağa bağlı tıbbi cihazlardaki güç tüketimi, bellek ve boyut kısıtlamaları göz önünde bulundurulmalıdır (Shah, 2019).

Kimlik Doğrulama ve Erişim Kontrolü: Kablosuz tıbbi cihazların güvenliği için kimlik doğrulama ve erişim kontrolü önlemleri kullanılmaktadır. Bu önlemler, yetkisiz erişimi engellemek ve sadece yetkilendirilmiş kullanıcıların cihaza erişimini sağlamak amacıyla tasarlanmıştır. Ancak, bu önlemleri uygulamada bazı zorluklar vardır. Asimetrik algoritmalar çoğunlukla komplike devreler

ve erişim izni vermek için karmaşık hesaplama ihtiyaçları ve yoğun iletişim kullanırlar, bu da asimetrik algoritmalar kullanan cihazın güç tüketimini artırır (Rathpre vd. 2017). Ayrıca kullanıcıların her seferinde parola girişi ve yetki kontrollerine vakit ayırmamak istemesi ve zayıf parolalar kullanması veya dikkatsiz kullanım sonucu yetkisiz kişilerin kimlik bilgilerini ele geçirmesi gibi sonuçlar doğurabilir. Bu nedenle, daha güçlü kimlik doğrulama yöntemlerinin ve erişim kontrolü politikalarının geliştirilmesi, uygulanması ve takibi önemlidir.

Veri Şifreleme: Kablosuz tıbbi cihazlarda veri şifrelemesi kullanılarak iletilen verilerin güvenliği sağlanır. Şifreleme, verilerin yetkisiz kişiler tarafından okunmasını engeller. Ancak, şifreleme algoritmalarının güvenliği ve güncelliği önemlidir. Eski algoritmalarda bulunan açıklıklar saldırganlar tarafından çok iyi bilindiğinden bu tip şifrelerin kolaylıkla kırılması veya arka kapı açıklıkları ile aşılması olasıdır. Yeni güvenlik tehditlerine karşı dayanıklı şifreleme yöntemleri ve protokollerinin kullanılması gerekmektedir. Verilerin şifrelenmesi güvenliği arttırırken veriler ulaşılabilirliğini olumsuz etkileyebilir. Tıbbi hizmet veren kurum çalışanlarının çalışmak istediği verilerde bir arama yapmadan evvel ilgili verilerin şifresini çözmesi gereklidir, dolayısıyla verilerin şifrelenmesi verilere ulaşılması ve verilerin işlenmesi için daha fazla emek, zaman ve maliyet isteyen bir işlem olarak görülür (Esposito vd. 2018).

Güncelleme ve Yama Yönetimi: Kablosuz tıbbi cihazların güvenlik açıklarını gidermek ve yeni tehditlere karşı korunmak için düzenli güncellemeler ve yamalar sağlanmalıdır. Bu, güvenlik açıklarının tespit edilmesi ve bunlara yönelik çözümlerin hızlı bir şekilde dağıtılması anlamına gelir. Ancak, eski donanımlara sahip cihazların güncel yazılımları desteklememesi, güncelleme ve yama yönetimi süreçlerinin karmaşıklığı, çok sayıda cihazın eş zamanlı güncellenememesi, hatta hangi cihazın hangi sürümde olduğunun takip edilememesi gibi sorunlar tıbbi cihaz üreticileri ve sağlık kuruluşları için zorluklar oluşturabilir.

Ağ Güvenliği ve İzleme: Kablosuz tıbbi cihazların bağlı olduğu ağların güvenliği önemlidir. Bu ağlara siber güvenlik konusunda yeterli eğitim farkındalığa sahip olmayan kullanıcı erişimlerinin kolaylaştırılması için gerekli güvenlik önlemlerinin tam olarak alınamaması ağa sızmayı kolaylaştırabilir.

Güvenlik Politikaları ve Prosedürler: Güvenlik politikaları ve prosedürler, genellikle fazla detaylı ve uygulaması zor görülerek uygulamada kullanılmayabilir. Tıbbi cihazların kullanıldığı ortamların hastaneler gibi genellikle halka açık olması bu alanların fiziksel güvenlik önlemlerinin alınmasını da zorlaştırmaktadır. Uygulanmayan güvenlik politikaları ile de siber saldırılara açık bir ortam oluşabilir.

SONUÇ VE ÖNERİLER

Bu makale, kablosuz tıbbi cihazlarda siber güvenlik konusunda tehditleri, önlemleri, uluslararası standartları ve örnek çalışmaları kapsamlı bir şekilde incelemektedir. Bulgularımız, kablosuz tıbbi cihazların güvenlik açıklarının ciddi risklere yol açabileceğini göstermektedir. Hasta verilerine sahip kablosuz ağa bağlı tıbbi cihazlar, saldırganların yeteneklerini kullanarak cihazları ele geçirebilmesine ve hastaların sağlığına zarar verebilmesine olanak tanır. Bu nedenle, kablosuz tıbbi cihazların siber güvenliği, sağlık sektöründe büyük bir endişe kaynağıdır.

Araştırmamız, kablosuz tıbbi cihazlardaki güvenlik zayıflıklarının çeşitli faktörlerden kaynaklandığını ortaya koymuştur. Bunlar arasında zayıf şifreleme yöntemleri, yetkilendirme ve kimlik doğrulama eksiklikleri, yazılım güncelleme süreçlerindeki aksaklıklar ve ağ trafiğindeki

güvenlik açıkları yer almaktadır. Bu zayıflıkların etkin bir şekilde ele alınması hem üreticilerin hem de sağlık hizmeti sağlayıcılarının sorumluluğundadır.

Bu çalışma ayrıca, kablosuz tıbbi cihazlarda siber güvenliği artırmak için öneriler sunmaktadır. Kablosuz tıbbi cihaz üreticilerinin, güvenlik önlemlerini cihazların tasarım ve geliştirme aşamalarından başlayarak entegre etmeleri gerekliliği vurgulanabilir. Yapay zekâ ve makine öğrenimi tekniklerinin kullanımıyla daha etkin ve dinamik güvenlik önlemleri oluşturulabilir. Güçlü şifreleme yöntemlerinin kullanılması, güvenlik yazılımının düzenli olarak güncellenmesi, ağ trafiğinin sürekli izlenmesi ve saldırı tespit sistemlerinin uygulanması, ayrıca kablosuz tıbbi cihazların güvenlik açıklarının belirlenmesi ve saldırılara karşı dayanıklı hale getirilmesi için daha kapsamlı test ve değerlendirme yöntemlerinin oluşturulması gerekmektedir. Kullanıcıların güvenlik konusunda eğitim alması ve farkındalıklarının artırılması da önemli bir adımdır.

Düzenleyici kurumlar ve endüstri, kablosuz tıbbi cihazlarda siber güvenliği teşvik etmek için iş birliği yapmalıdır. Standartlar ve yönetmelikler, güvenlik gereksinimlerini belirlemek ve uygunluk değerlendirmelerini sağlamak için güncellenmelidir. Ayrıca, sağlık sektöründe çalışanların ve hastaların siber güvenlik konusunda eğitim almaları ve bilinçlenmeleri önemlidir.

Sonuç olarak, kablosuz tıbbi cihazlarda siber güvenlik, sağlık sektöründe büyük bir öneme sahip bir konudur. Bu alanda daha fazla araştırma ve geliştirme çalışmalarına ihtiyaç vardır. Üreticiler, sağlık hizmeti sağlayıcıları, düzenleyici kurumlar ve diğer paydaşlar arasında iş birliği ve bilgi paylaşımı, güvenlik önlemlerinin etkin bir şekilde uygulanması için kritik öneme sahiptir. Siber güvenlik önlemlerinin uygulanması, denetlemesinin önemi kadar bunun ilgili tüm paydaşlarda bir yaşam tarzı, kültür haline gelmesi sorunun çözüme kavuşması için önemli mesafe kat edilmesini sağlayacaktır. Bu çalışmanın sonuçları, kablosuz tıbbi cihazların güvenlik açıklarının anlaşılmasına ve daha güvenli sağlık hizmetlerinin sunulmasına katkı sağlamak için alınması gereken adımların netleştirilmesine yardımcı olacaktır.

Araştırmacıların Katkı Oranı: Yazarların çalışmadaki katkı oranları eşittir.

Çatışma Beyanı: Çalışma kapsamında herhangi bir kurum veya kişi ile çıkar çatışması bulunmamaktadır.

KAYNAKÇA

Alsubaei, F., Abuhussein, A., Shandilya, V., ve Shiva, S. (2019). IoMT-SAF: Internet of medical things security assessment framework. Internet of Things, 8, 100123. https://doi.org/10.1016/j.iot.2019.100123

Coventry, L., ve Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, 113, 48-52. https://pubmed.ncbi.nlm.nih.gov/29903648/

Deloitte. (2013). Networked medical device cybersecurity and patient safety: Perspectives of health care information. Deloitte. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/life-sciences-healthcare/us-lhsc-networked-medical-device.pdf

Denning, T., Fu, K. ve Kohno, T. (2008) Absence makes the heart grow fonder: New directions for implantable medical device security. In HotSec.

Esposito, C., Santis, A., Tortora, G., Chang, H. ve Choo, K. (2018) Blockchain: A panacea for healthcare cloud-based data security and privacy? IEEE Cloud Computing, 5(1):31–37, 2018

Garcia. (2017). Why cybersecurity must be part of medical device architecture. Medical Device and Diagnostic Industry Qmed. https://www.mddionline.com/

Gollakota, S., Hassanieh, H., Ransford, B., Katabi, D., Fu K. (2011) They can hear your heartbeats: non-invasive security for implantable medical devices. In Proceedings of the ACM SIGCOMM conference, pages 2–13, 2011.

Harit, H., Ezzati, A., & Elharti, R. (2017). Internet of things security: Challenges and perspectives.ICC'17: Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing (ICC '17),167, 1-8. https://doi.org/10.1145/3018896.3056784

HHS. (2021). 2020: A retrospective look at healthcare cybersecurity. Department of Health and Human Services. Leadership for IT Security & Privacy across HHS. HHS Cybersecurity Program. Office of Information Security. https://www.hhs.gov/sites/default/files/2020-hph-cybersecurty-retrospective-tlpwhite.pdf

HIPAA Ransomware. (2017). Wannacry ransomware encrypted hospital medical devices. HIPAA Journal.com. https://www.hipaajournal.com/wannacry-ransomware-encryptedhospital-medical-devices-8811/

Kovacs, E. (2014). 70 percent of iot devices vulnerable to cyberattacks: HP. Security Week. https://www.securityweek.com/70-iot-devices-vulnerable-cyberattacks-hp.

Laurinda B Harman, Cathy A Flite, and Kesa Bond. Electronic health records:privacy, confidentiality, and security. AMA Journal of Ethics, 14(9):712–719, 2012.

Li, H., Sun, G., Li, Y., & Yang, R. (2021). Wearable wireless physiological monitoring system based on multi-sensor. Electronics, 10(9), 986. https://doi.org/10.3390/electronics10090986

Maras, M.-H. (2015). Internet of Things: Security and privacy implications. International Data Privacy Law, 5(2), 99–104. https://doi.org/10.1093/idpl/ipv004

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: How safe are we. BMJ. https://doi.org/10.1136/bmj.j3179

McFarland, R. J., & Olatunbosun, S. B. O. (2019). An exploratory study on the use of internet of medical things (iomt) in the healthcare industry and their associated cybersecurity risks. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp). https://csce.ucmss.com/cr/books/2019/LFS/CSREA2019/ICM2519.pdf

Miraz, M. H., Ali, M., Excell, P. S., & Picking, R. (2018). Internet of nano-things, things and everything: Future growth trends. Future Internet, 10(8), 68. https://doi.org/10.3390/fi10080068

Morgan, S. (2019). Patient insecurity: Explosion of the internet of medical things: How vulnerable is the iomt to cyber threats? CyberCrime Magazine. 119 https://cybersecurityventures.com/patient-insecurity-explosion-of-the-internet-ofmedical-things/

Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., Alabdulatif, A., Alshoura, W. H., & Arshad, H. (2021). The internet of things security: A survey encompassing unexplored areas and new insights. Computers & Security, 102494. https://doi.org/10.1016/j.cose.2021.102494

Rathpre, H., Mohamed, A., Al-Ali, A., Du, X., ve Guizani, M. (2017). A review of security challenges, attacks and resolutions for wireless medical devices. In 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), pages 1495–1501. IEEE, 2017.

Sağlık Bakanlığı, (2019). Tıbbi Cihazlarda Alınması Gereken Güvenlik Önlemleri Dokümanı V.1.0 https://some.saglik.gov.tr/Eklenti/42923/0/tibbi-cihazlarda-alinacak-guvenlik-onlemleri-dokumani-v.docx

Schumaker, E. (2020). Elon musk unveils brain chip implant: It's like a fitbit in your skull. ABC News (online). https://abcnews.go.com/Health/elon-musk-unveils-brain-chip-implantfitbit-skull/story?id=72703840

Shah, K., (2019). Privacy and Security Issues of Wearables in Healthcare. Doktora Tezi, Flinders University, College of Science and Engineering.

Steger, A. (2020). What makes iomt devices so difficult to secure? HealthTechmagazine.net. https://healthtechmagazine.net/article/2020/02/what-makes-iomt-devices-so-difficultsecure-perfcon

Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S., & Wang, G. (2018). Security and privacy in the medical internet of things: A review. Security and Communication Networks, 2018, 5978636. https://doi.org/10.1155/2018/5978636

Thielfoldt K. (2022). Internet of Medical Things Cybersecurity Vulnerabilities and Medical Professionals' Cybersecurity Awareness: A Quantitative Study

TrapX Research Labs. (2021). TrapX Anatomy of attack: MEDJACK.2: Hospitals under siege. https://www.trapx.com/wpcontent/uploads/2021/01/AOA_Report_TrapX_MEDJACK.2.pdf

Tsiatsis, V., Karnouskos, S., Holler, J., Boyle, D., & Mulligan, S. (2018). Internet of Things: Technologies and Applications for a New Age of Intelligence. Academic Press.

Xu, F., Qin, Z., Tan, C., Wang, B., Li, Q. (2011) Imdguard: Securing implantable medical devices with the external wearable guardian. In 2011 Proceedings IEEE INFOCOM, pages 1862–1870. IEEE, 2011.

Zhenge, J., Shen, Y., Zhang, Z., Wu, T., Zhang, G., & Lu, H. (2013). Emerging wearable medical devices towards personalized healthcare. BodyNets '13: Proceedings of the 8th International Conference on Body Area Networks, 2013, 427-431. https://eudl.eu/doi/10.4108/icst.bodynets.2013.253725