TIBBİ SİSTEMLERİ VE CİHAZLARI HEDEF ALAN SİBER SALDIRILAR

CYBER ATTACKS TARGETING MEDICAL SYSTEMS AND DEVICES

İ. Hamit HANCI[1]
Hilal TOKGÖZ[1]
İshak YAPAR[2]

Adli Bilimler Dergisi / Turkish Journal of Forensic Sciences, 17 (1): 32 - 39; 2018

ÖZET:

Bilgisayar sistemleri günümüzde birçok fayda sağlamaktadır. Yeni yazılımlar ve sistemler sağlık sektöründe yaygın olarak kullanılmaktadır. Ama bu sistemlerde birçok güvenlik problemi bulunmaktadır. Medikal cihazlara siber saldırı riski devamlı artmaktadır. Sadece pazarlama öncesi kontrollerle bu riski tamamen azaltmak mümkün değildir. Sağlık sektörleri güvenlik davranışlarını ve risk değerlendirmelerini yapmalı ve sonrasında olay plan geliştirmelidirler.

Anahtar Kelimeler: Siber Saldırı, Medikal Sistem, Medikal Cihaz.

ABSTRACT:

Nowadays computer systems provide many benefits. New software and systems are used more widely in healthcare systems. However, these systems have many security problems. Risks of cyber-attacks to medical devices increase continuously. It is not possible to reduce this risk completely only by controls just before marketing. Healthcare organizations should conduct security frameworks and risk assessments and then develop new plans.

Keywords: Cyber-Attack, Medical System, Medical Device.

GİRİŞ

Bilgisayar sistemleri her geçen gün daha fazla gelişmekle birlikte gün geçtikçe yaşamın her alanının vazgeçilmez bir parçası haline gelmektedir. Bu gelişmeler çok sayıda yarar ve kolaylık sağladığı gibi güvenlik tehdidini de beraberinde getirmektedir. Yeni yazılımlar ve sistemler tüm sektörlerde olduğu gibi sağlık alanında da çok yaygın ve sık olarak kullanılmaktadır. En başta ulusal sağlık programları ve sistemleri başta gelmek üzere, hastane kayıt ve bilgi sistemleri, hasta reçeteleri, tedavi protokolleri, tetkik istemleri ve sonuçları bilgisayar yazılımları ve sistemleri üzerinden yapılmaktadır. Ayrıca tüm tedavi ve tetkik cihazları da bilgisayar yazılımları ve sistemleri aracılıyla kullanılır hale gelmiştir (1).

Bilgisayar sistemlerinin sağladığı yararların yanı sıra bu bilgisayar sistemleri ve yazılımlarının alt yapısındaki boşluklardan yararlanılarak hackerlar (bilgisayar korsanları) tarafından bu bilgilere ulaşılabilir (2). Hackerlar; bilgisayar sistemleri konusundaki bilgisini gizli bilgilere ulaşmak, ağlar aracılığıyla yasal olmayan zarar verici saldırılar yapmak yani siber saldırılar için kullanan kimselerdir (3). Sağlık merkezlerine yapılan siber saldırılar veri kaybına yol açmak, parasal hırsızlık yapmak, tıbbi cihazlara saldırı yapmak ve altyapıya saldırı yapmak olarak dört farklı grupta incelenebilmektedir (4).

Sağlık sektöründeki veriler en az finans, enerji ve askeri veriler kadar tehlike altındadır. Yapılan son araştırmalara göre sağlık merkezlerinin %94 kadarı bu siber saldırıların kurbanı durumundadır (5). Sağlık hizmet sunucularının hasta veri güvenliğini sağlama konusunda alt yapılarında çok sayıda engel söz konusudur. Bir taraftan bilişim sektörünün çok hızlı gelişmesi ve yapılan sistemlerin güvenlik konusunda yeterli olamaması ciddi zorluklara yol açmaktadır. Institute for Critical Infrastructure Tecnology (Kritik Altyapı Teknoloji Enstitüsü)'nin hazırladığı rapora göre sağlık sektörü ABD'de en fazla siber saldırı tehdidinde olan ama en az hazırlıklı olan alandır (6). ABD'de yapılan bir anket çalışmasına göre sağlık alanındaki üst düzey yetkililerin siber güvenlik konusundaki en büyük korkuları sistemlere yada tıbbi cihazlara yetki dışı erişen kötü niyetli kişilerden dolayı

[1] Ankara Üniversitesi, Tıp Fakültesi, Adli Tıp Anabilim Dalı, Ankara
[2] Çalışma ve Sosyal Güvenlik Bakanlığı Yurtdışı İşçi Uzmanı, Bilgisayar Mühendisi, Ankara

hasta bilgilerinin kaybedilmesi yada değiştirilmesidir. Uygulama yazılımları güvenlik şirketi olan Veracode'un yaptığı bir ankete göre artan güvenlik ihlallerinden sağlık çalışanları ciddi anlamda kaygı duymaktadır. Ankete katılan 200'den fazla hastane ve sağlık bilişim yetkilisi katılımcının %28 kadarı başlıca kaygılarının hackerların elektronik sağlık kayıt sistemleri ve medikal cihazlardaki açıkları kullanmaları olduğunu ifade etmiştir (7).

Siber güvenlik uzmanları hacklenme ihtimali daha yüksek olan; bilgisayar chipi, yazılımı, kablosuz ağ teknolojisi ve internet bağlantısı olan tıbbi cihazlar ve hastane ekipmanı üzerinde yaptıkları çalışmalar sonucunda hayati tehlike oluşturabilecek hatalar tespit etmişlerdir (8). Medikal cihaz yazılımları, bağlı olduğu sistemlerinde güvenlik açıkları oluşturarak hasta güvenliğini riske atacak saldırılara zemin hazırlayabilirler.

Araştırma şirketi Forrester siber güvenliğe dair raporunda internete bağlı cihazların yaygınlaşmasıyla siber saldırıların hedefinde özellikle medikal cihazların olacağını belirtmektedir. Örnek olarak, ameliyatsız gerçekleştirilen ve kablosuz iletişim sistemiyle ulaşım sağlanabilen kalp pilinin bağlantısına müdahale edebilen bir hacker fidye almak için ölümle tehdit edebilir. Düzenlenen rapora göre teknolojik gelişmelerle 2016 yılının bu şekilde saldırılar için bir başlangıç yılı olacağını belirtmektedir. Sağlık sektöründe çalışanların bugüne kadar medikal cihazlara yönelik saldırılarla çok sık karşılaşmadıkları için, siber saldırılar konusunun üzerinde çok durmadıkları görülmektedir. Sağlık cihazlarında genellikle fabrikada yapım aşamasında belirlenen ve kullanıcı müdahalesiyle değiştirilemeyen sabit kodları bulunmaktadır. Bu şifrelerin ele edilmesiyle, çok sayıda hastanın siber saldırganların eline düşme tehlikesi vardır (9).

GERÇEKLEŞTİRİLEN VE OLASI SALDIRILAR

- Amerika Bileşik Devletleri Gıda-İlaç İdaresinin 2015 yılında cihazlar üzerinde yaptığı bir araştırmada Hospira Life Care PCA3 ve PCA5 bilgisayarlı infüzyon pompa sistemlerine hackerlar tarafında kablolu veya kablosuz ağ kullanılarak uzaktan erişilebileceğini ve verilen ilaç dozlarında değişim yapılabileceğini belirtmiştir. Cihazlardaki güvenlik boşluklarının ortadan kaldırılması için çeşitli önerilerde bulunmuştur (10).
- ABD'de doktorun uyguladığı ilaçların takibi için kullanılan sistemdeki teknik hataları tespit eden bir hemşire sistemdeki açığı kullanarak 2006 yılında yakalanana kadar 16 yılda en az 40 hastayı ölümüne neden olduğunu kabul etmiştir. Fakat uzmanlar cinayet sayısının 400 civarında olduğunu tahmin etmektedir (11).
- Gerçek hayatta, savaş esnasında askerleri hastanelere saldırı yapılmamaktadır. Ama hackerlar tarafından bu tarz saldırılar yapılabilmektedir. Boston hastanesi Beth Israel Deaconness CIO'su John Halamka 24 saat içinde her 7 saniyede bir saldırıya uğradıklarını belirtmektedir. Halamka, Micgihan Üniversitesinde medikal cihaz güvenlikleri üzerinde çalışan mühendislik profesörü Kevin Fu ile birlikte medikal siber saldırılar panelinde bir araya geldiklerinde geçmiş yıllarda gerçekleşen büyük hastanelere karşı yapılan siber saldırılardan bahsetmişlerdir. Bir hastanenin başına gelebilecek olası siber saldırıları bir araya getirerek; bu panelde özellikle medikal sistemlere ve cihazlara yönelik yapılan saldırılara dikkat çekmişlerdir. Panelde daha önce gerçekleştirilen beş siber saldırıyı örnek göstermişlerdir.

1) Kayıtların çalınması (Çin): Hastanelerdeki çoğu bilgisayar ya da medikal cihazlar çok sayıda güvenlik açığı bulunan eski sistemlerle çalışmaktadır. Hastaneler bu cihazları internet ağına bağlamaktan kaçınmaktadırlar. Beth Israel Deaconess Hastanesi medikal kayıtlarını bilgisayarda saklayarak önlem almaktaydı. Ancak bilgisayarların yazılım güncellemesine ihtiyacı olduğunda üretici firma tarafından hastaneye bir teknisyen yollamıştır ve teknisyen güncellemeyi indirebilmek için bilgisayarları internete bağlamıştır ve öğle yemeği için ara vermişlerdir. Teknisyen

geri döndüğünde ise bilgisayarlar çoktan virüslerle dolmuş ve artık çalışamayacak durumdadırlar. Bilgisayarlar aracılığıyla 2000'den fazla hastanın kişisel X-ray kayıtları çalmıştır. Çin'de tüberküloz gibi bulaşıcı akciğer hastalıkları olduğu için vize alamayan kişiler çalınan X-ray kayıtlarını vize alabilmek kullanmışlardır.

2) Kimliği belirsiz kişiler tarafından gerçekleştirilen DDoS atakları: 2014 yılında Boston Çocuk Hastanesi, devlet gözetimi altına alınan bir genç kızla ilgili tartışmalı bir davayla uğraşmaktaydı. Doktorların iddiasına göre genç kızın hastalığı büyük ölçüde psikolojikti ve ailesi gereksiz tedavilerin uygulanmasında ısrarcıydı. Bir hacker grubu genç kızın haklarının ihlal edildiği gerekçesiyle hastaneyi DDoS atağıyla cezalandırmaya karar verdi. DDoS saldırısı birçok kaynaktan hedefin erişilebilirliğine yapılan saldırılardır. Saldırılarda, sistemin kaldırabileceği yükten fazla anlık istek, anlık kullanıcı sayısı ile sistem cevap veremez hale getirilir. DDoS'un en tehlikeli yanı saldırıyı gerçekleştirmek için üst düzey teknik bilgiye gereksinim olmamasıdır. Öyle ki internetten indirilen basit programlar aracılığıyla bir sisteme yönelik saldırı yapılabilir ve sadece IP adresi veya bölüm adı girilerek hedef sistemin erişim dışı olması sağlanabilmektedir. Ama hacker grubunun saldırısı istenilenden daha büyük ölçüdeydi çünkü hastanenin IP adresini bilmiyorlardı ve ellerinde IP adresi olmadığı için saldırıyı gerçekleştirmek için bölgenin tüm internet ağına saldırmışlardır. Harvard üniversitesi dahil bölgedeki tüm hastaneler erişime kapalı hale gelmiştir.

3) Sahte Doktor Taklidi: Sahte siteler neredeyse aslından ayırt edilemeyecek derecede mükemmel şekilde taklit edilmektedir. "Mass General Hastanesi"nin sahte personel portalı gerçeğiyle neredeyse aynı yapılmıştır. Doktorlar bu sayfadan ekstra ödeme ile ilgili bilgilendirici bir mail aldıklarında çoğu linki memnun bir şekilde takip etmiştir. Linke tıkladıktan sonra hepsi kimlik bilgilerinde bir yanlışlık olduğunu fark etmeden sisteme giriş yapmışlardır. Hackerlar bu bilgilerle gerçek sistemdeki doktorların mevduat bilgilerini değiştirmişlerdir. Yasa dışı olarak elde ettikleri paraları ise internet alışverişi yapılan bir siteden hediye kartı almak için kullanmışlardır. Hastane yetkilileri artık sadece şifreyle girilen online ödeme istemini kullanmadığını, daha fazla önlem alma yoluna gittiklerini belirtmektedirler.

4) Angry Birds Tuzağı: Beth Israel Deaconess Hastanesinde çalışan bir hemşire sadece biraz eğlenmek için Angry Birds oyununu Android telefonuna indirmiştir. Ne yazık ki uygulamayı, uygulamayla birlikte kötü amaçlı yazılım da indiren bir siteden indirmiştir. Daha sonra, hemşire telefonuyla iş mailine giriş yaptığında, ekran kopyalama programı hemşirenin giriş bilgilerini kaydetmeye başlamış ve sonuç olarak hemşirenin hesabı Harvard.edu tarafından 1 milyon spam mesajı yollamak için kullanıldı. Bu da Verizon'un Harvard'ı 'spammer' olarak bloklamasına yol açtmıştır.

5) Ya tamamını öde yoksa ..?: Hastaneler üzerindeki fidye saldırıları büyüyen bir tehdit olarak görülmektedir. Bu tip saldırılarda hackerlar bilgisayar ağını gasp etmekte, şifrelemekte ya da bilgisayarın bilgilere erişimini engellemektedirler. Daha sonra erişimini engellediği bilgileri iade etmek için fidye talep etmektedirler. Bu saldırganlar özellikle belirli kişileri ve önemli kuruluşları hedef almaktadır. Hedef hastaneler olduğunda, bilgi erişiminin kapalı olduğu zaman zarfı içindeki hizmet verememenin getirdiği tepkilerin boyutu oldukça büyük olmaktadır. Birçok hastane bu tarz saldırılara uğramış ve ödeme yapmak zorunda kalmıştır. Los Angeles'daki Hollywood hastane ağı saldırganlar tarafından ele geçirilmiş ve 3 milyon dolar ödeme istediklerinden dolayı 1 hafta boyunca devre dışı kalmıştır.

- Daha önceleri nadir olan siber saldırılar artık sağlık sisteminde de rutin bir saldı-

rı şekline dönüşmüştür. Artan siber saldırılara rağmen hastaneler siber güvenlik için ayrı bir bütçe oluşturmamaktadır. Halamka "sağlık hizmetlerinde, bilgi teknolojilerine bütçenin %2'sini harcıyoruz ve güvenlik bunun %10'u civarında olduğunu belirtmiştir. Rakamları karşılaştırmak gerekirse finansal şirketler bütçelerinin %35'ini bilgi teknolojilerine harcamaktadır" (12). Sektörlerin güvenliğe ayırdığı bütçedeki bu farklılıklar sağlık sisteminde hala güvenliğin çok fazla dikkate alınmadığını göstermektedir.

- Medikal implante cihazlar (pacemaker, implante kardiak defibrilatör (ICD), ilaç alım sistemleri, nörostimülatör vb.) güvenlik açısından önemlidirler. Bu cihazlara wireless (kablosuz ağ) ile ulaşım sağlanabildiği çalışmalarda gösterilmiştir. Bu cihazlara yönelik saldırılar sonucu kişilerin hayati tehlikesi oluşabilmektedir (13).
- TC Sağlık Bakanlığı'nın 18 Mayıs 2016'da yapıldığı iddia edilen siber saldırı ile ilgili yazılı olarak yaptığı resmi açıklamaya göre; Sağlık Bakanlığına bağlı hastanelere yönelik siber saldırı girişimiyle ilgili açıklama yapılmasına gerek görülmüştür. Bakanlığa bağlı Diyarbakır, Siirt, Tekirdağ ve Kocaeli illerinde bulunan bazı hastanelere yönelik bir siber saldırı girişimi olmuştur. Siber saldırıdan sadece Diyarbakır ilindeki hastaneler kısmen etkilenmiş olduğu tespit edilmiştir. Bilgi sistem altyapısındaki yedekleme mekanizmasıyla veri kayıplarının önüne geçilmiştir. Saldırı sonrası hastanelerin bilgi sistemlerindeki aksamalar kısa sürede giderilmiştir. Sağlık hizmetlerinde mağduriyet yaşanmasını önüne geçilmeye çalışılmıştır. Veri güvenliğini tehdit eden bu saldırı girişimiyle ilgili inceleme başlatılmıştır. Bakanlığa bağlı sağlık kuruluşlarının bilgi sistemleri güvenlik altyapılarıyla korunmaktadır. Bu amaçla "Sağlık Bilişim Özel Ağı" oluşturulmuştur. Bu ağ ile birlikte sağlık tesislerinin internet erişimi güvenli olarak gerçekleştirilmesi hedeflenmektedir. Bakanlığa bağlı tüm sağlık tesislerinin bu ağa dahil edilmesiyle ilgili altyapı çalışmaları hızla devam etmektedir" (14). Bakanlık tarafından yapılan bu açıklamaya göre Türkiye'deki sağlık sistemlerinin de saldırılara maruz kaldığı görülmektedir.
- Medtronic'e sızılması sağlık verileri çalınması; Dünyanın en büyük medikal cihaz üreticilerinden Medtronic, siber saldırı sonucunda bazı hastaların kayıtlarını kaybettiklerini duyurmuştur. Şirket sisteme izinsiz bir giriş yapıldığının farkına vardıklarını açıklamışlardır. Saldırganların hastalarla ilgili bilgilerin depolandığı veritabanına sızamadığını açıklayan Medtronic, bazı şeker hastalarının kayıtlarının ortadan kaybolduğu bilgisini vermiştir. Çalınan bu hasta kayıtlarında ne gibi bilgilerin yer aldığı açıklanmamıştır. Şirketin Amerikan Sağlık Hizmetleri Departmanı tarafından veri güvenliği konusunda soruşturmaya tabi tutulacağı açıklanmıştır (15).
- Billy Rios (Bilgi Güvenliği Uzmanı) rahatsızlığı nedeniyle hastanenin acil servisine başvurmuştur. Acil serviste kullanılan otomatik ilaç pompaları önceden yürüttüğü bir güvenlik araştırması çalışmasından hatırlaması bilgi güvenlik uzmanının tedirgin olmasına neden oldu. Bilgi Güvenliği Uzmanını o anki acil rahatsızlığından çok, onu bağlayacakları ilaç pompasının siber saldırıya uğrama ihtimali endişelendirmekteydi. Uzmanın cihazda saptadığı güvenlik boşluğu internet üzerinden pompa müdahale edilerek ilaç dozu miktarlarının değiştirmesine izin vermekteydi. Güvenlik boşluğundan faydalanmak isteyen bir hacker pompanın ilaç dozlarını değiştirerek ölümcül dozlarda ilaç verilmesiyle hastaların ölümüne sebep olabilirdi. Medikal cihaz güvenliği ile ilgili çalışma yapan başka araştırmacılar da internet üzerinden ulaşılabilir ve sistemleri değiştirilebilir medikal cihazlar olarak insülin pompalarını, defibrilatörleri ve çeşitli tıbbi cihazları saptamışlardır. 2011 yılında Radcliffe adlı bir araştırmacı çok az para harcayarak basit bir sistem kurarak insülin pompalarının

ilaç dozlarının uzaktan erişimle ayarlanabileceğini göstermiştir ve sonrasında kalp pili, radyoloji cihazları ve diğer benzeri medikal kadar pek çok tıbbi cihaz için yeni saldırı yöntemleri ortaya çıkmaktadır. Radcliffe tarafından saptanan güvenlik açığı ise, cihazın hastane sistemiyle kurduğu iletişim sistemine müdahale ederek, sistemden alması gereken gerçek güncelleme verisi yerine hacker tarafından gönderilen sahte güncelleme bilgisinin cihaza yüklenmesine olanak vermesidir. Bu yöntemle hacker pompanın üzerinde bulunan ve müdahalelere karşı bir miktar koruma sağlayan yazılıma müdahale etmek yerine bu pompaları merkez üzerinden yöneten yazılıma müdahale ederek saldırı yapabilmektedir. Billy Rios, dünya genelinde 55,000'den fazla hastanede kullanımda olan bir ilaç pompalarını yöneten yazılımda 4 farklı güvenlik açığı saptamıştır. Saptadığı yazılım sistemi güvenlik açıklarının yanı sıra sistem güncellemeleri için kullanılan işlemlerde de önemli açıklar tespit etmiştir. Telefonlarda güncelleme yüklenirken güncellemenin kaynağını ve indirilen güncelleme dosyasının içeriğini kontrol etmesini sağlayan önlemler vardır ve bu güvenlik denetimi sayesinde "uygulama güncellemesiymiş gibi" zararlı yazılım gönderme olanağı bulunmamaktadır. Rios'un araştırmalarında yazılımda saptadığı güvenlik açıklarında bu şekilde bir kontrolün olmadığını görmüştür. Güvenlik açıkları sayesinde "güncelleme" dosyası gibi görünen bir zararlı yazılımlarla pompanın yönetim sistemini ele geçirebilmektedir. Kardiyoloji, onkoloji ve birçok bölümde kullanılan başka medikal cihazların da hastane yönetim sistemleri ile bağlantılı halde (güncelleme, ilaç dozu, tedavi planı veya hasta bilgisi gibi verileri gönderip aldığı) çalışmasıyla medikal cihazların güvenliği konusunda tartışmalara neden olmaktadır. Amerika Bileşik Devletleri İç Güvenlik Bakanlığı 20'den fazla medikal cihazın saldırganlar tarafından ele geçirilebilmesi tehlikesi nedeniyle araştırma çalışmaları başlatmıştır. Kimliği gizli bakanlık yetkilisinin açıklamasında, yapılan araştırma çalışmalarının siber saldırı ihtimali nedeniyle başlatıldığını söylemiştir. Medikal cihazlara saldırı konusunda akla gelen en sık örneklerden bir tanesi de 2007 yılında, dönemin Amerika Birleşik Devleti Başkan Yardımcısı olan Dick Chenney'in kalbine takılı kalp pilinin kablosuz erişim özelliğinin devreden çıkartılmasıdır. Bu olay birçok film senaryolarına da eklenmiştir ve medyada geniş yer bulmuştur (16).

ALINAN ÖNLEMLER VE ÖNERİLER

Son dönemlerde, FDA tıbbi cihaz siber güvenliğine yönelik Tıbbi Cihazların Siber Güvenliği Konusunda Pazarlama Sonrası Yönetim adlı bir taslak kılavuz yayımlamıştır. Bu kılavuz Tıbbi Cihazların Siber Güvenliği İçin Pazarlama Öncesi Sunumların İçeriği adlı kılavuzun devamıdır ve Ağ Bağlantısı İçeren 150 Medikal Cihazın Siber Güvenliği için Yazılım adlı kılavuzu tamamlayıcı niteliktedir. Ayrıca IEEE Cybersecurity (Siber Güvenlik İnsiyatifi) tarafından da yazılım geliştirme sürecinde tıbbi cihaz güvenliğine yönelik Building Code for Medical Device Software Security (Tıbbi Cihazların Güvenli Yazılımı İçen Kod Oluşturma) adlı bir kılavuz yayınlamıştır (17-20).

Bu klavuzlarda yapılan araştırma ve incelemeler sonucunda medikal cihazlardaki güvenlik açıkları ve alınması gereken önlemler üzerinde durulmaktadır.

ABD'de yürürlüğe giren Siber güvenlik Bilgi Paylaşım Yasası, ABD Department of Health and Human Services (İnsan ve Sağlık Bakanlığı) tarafından bir siber güvenlik görev kuvveti oluşturmasını zorunlu kılmaktadır. Bu görev kuvveti;

- Siber güvenlik saldırılarına karşı özel sağlık kuruluşlarının kendi güvenliklerini sağlamada karşılaştıkları güçlükleri analiz edecek,
- Ağdaki tıbbi cihazları elektronik sağlık kayıtlarına bağlayan yazılımların güvenliğini sağlamada kuruluşların zorluklarını gözden geçirecek,

- Tehditleri değerlendirme bu tehditler için karşı alınacak önlemlere yönelik bilgileri HHS sekreterliğine bildirecektir (21).

Bilgisayar teknolojilerinin giderek sağlık sektöründe de vazgeçilmez hale gelmesiyle bu konuda bazı güvenlik önerileri yayınlanmıştır;

- Yönetim kuruluna bilgi güvenlik sorumlusu da dahil edilmelidir.
- Sistemlere koruma kalkanları oluşturulmalıdır. Yani, verilerin veri tabanında şifrelenerek korunması, koruma duvarı, saldırı tespit ve önleme sistemleri, fiziksel ve mantıksal erişim kontrolü vs.
- Risk değerlendirmesi yapmak için kurum içi çalışanlardan ziyade dış personelden yararlanılmalıdır. Böylece objektif sonuçlar alınabilmektedir.
- Sıkı güvenlik standartları gerektiren verilerin korunmasında bulut ortamını değil kurum içi depolama birimi kullanılmalıdır.
- Uygulama geliştirirken Open Web Application Security Project (OWASP) standartlarını takip edilmelidir. Güvenlik risklerini anlamada ve karar almada yardımcı olabilmektedir.
- Çalışanlar eğitilmelidir. E-posta ile yapılan saldırılarda hedef genellikle çalışanlardır ve bu konuda tedbirli olmaları gerekir. Çalışanlar "tanımadıklarından gelen e-posta eklerini açmamaları" konularında uyarılmalıdır.
- Veri güvenliğine ilişkin kurumlar taahhütlerine uygun bir güvenlik ortamı oluşturmalıdırlar (22).

Tıbbi cihazların rutin yazılım güncellemeleri için genellikle FDA onayı ihtiyaç duyulmamaktadır. Üretici firmaların sektördeki tehdit ve risklere karşı önlem almaları için siber güvenlik bilgi paylaşım ve analiz organizasyonlarına katılması gerekmektedir. Ayrıca, ürünlerin pazarlama sonrasındaki siber güvenlik risklerini yönetebilmek için, firmalar sistematik risk ve kalite yönetim sistemlerine sahip olmalıdırlar.

IBM'in hazırladığı Sağlık Koruma Endüstrisinde Güvenlik Eğilimleri raporunda sağlık kurumlarına sağlık bilgilerini korumak ve güvenliğini sağlamak amaçlı bazı önerilerde bulunulmaktadır. Bu önerilerden en önemlisi firmanın güvenlik stratejisi ve bütçe idaresi için Bilgi Güvenliği Şefinin işe alınmasıdır. Raporda tıbbi cihazlarda güvenlik boşlukları oluşturularak siber saldırılara zemin hazırlanabileceği belirtilmektedir. Cihazların güvenlik güncellemeleri önemlidir; bu cihazlar sağlık kurum ve kuruluşlarının ağ sistemine dahil edilmeden önce güvenlik değerlendirmesinin ve testlerinin mutlaka yapılması gerekmektedir, ağdaki cihazlara yetkisiz erişimler kısıtlanmalıdır, güvenlik açıklarının tespiti amaçlı sistemler ve cihazlar düzenli aralıklarla gözden geçirilmelidir. Güvenlik personelleri ağda yetkisiz erişimleri takip etmeli, cihaz denetimi, implante edilenler dahil tüm tıbbi cihazların erişilebilirlik testleri mutlaka yapılmalıdır. Raporda giriş kodları dahil şifrelemenin önemi vurgulanmaktadır. Siber saldırılardan korunmak amaçlı sağlık kurumlarının güvenlik stratejileri ve risk değerlendirme planları olmalı ve bu planların uygulanması sağlanmalıdır (23).

Ülkemizde siber saldırıları engellemek için sağlık sisteminde yeni yapılanma çalışmaları devam etmektedir. Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğünün pilot olarak birkaç bölgede başlattığı ve daha sonrasında tüm illeri kapsayacak olan 'Sağlık Bilişim Ağı Projesi' ile kurumsal yazışmalar, Elektronik Belge Yönetim Sistemi (EBYS), kurumsal elektronik posta, dosya paylaşımı ve ulusal ölçekli projelerin hızlı ve güvenli bir ağ üzerinden, izlenebilir ve yönetilebilir bir yapıda işletilmesi planlanmaktadır. İnternet çıkışlarında güvenlik önlemlerini sağlamak amacıyla sistematik bir düzenleme yapılarak proje kapsamındaki illerin internete çıkışlarının Bakanlık Merkezinden kontrollü olarak yapılması düşünülmektedir (24).

TARTIŞMA-SONUÇ

Bilgisayar sistemlerinin sürekli olarak hızlı bir şekilde gelişmesiyle birlikte kullanım alanları giderek artmış durumdadır. Sağlık sis-

temleri ve medikal cihazlarda da giderek artan oranlarda bilgisayar sistemleri kullanılmaktadır. Bu durum birçok açıdan kolaylık sağladığı gibi bilgisayar sistemleri üzerinden yapılabilecek saldırılara da zemin hazırlamaktadır.

Sağlık sistemi ve cihazlarının pazara sürülmeden önce kontrollerden geçirilerek muhtemel risklerinin analiz edilmesi saldırı risklerini azaltmak için önemli ancak yeterli olmadığı yapılan araştırmalarda da görülmektedir. Teknolojinin gelişmesiyle birlikte yeni güvenlik açıkları tespit edilmektedir. Bu güvenlik açıklarından faydalanılarak yapılabilecek saldırılar stratejik öneme sahip kurumlara ve kişilere yönelik olma ihtimali vardır.

Tüm bu değerlendirmeler sonucunda sağlık sektörünün aslında siber saldırıya çok açık olduğu ancak yeterli güvenlik öneminin verilmediği ve önlem için yeterli bütçenin ayrılmadığı görülmektedir. Bu saldırıların önlenmesi konusunda üretici firmaların risk ve tehditlere yönelik yeni stratejiler geliştirmeleri gerekmektedir. Alınan tedbirlerin standartlaştırılması ayrıca yeni gelişen teknolojilere yönelik sistemlerinin güncellenmesi gerekmektedir. Ayrıca bu alınan önlemlerin uygulanıp uygulanmadığı, gerekli güncelleme ve yenileme çalışmalarının yapılıp yapılmadığı da devlet kontrolünde çeşitli kurumlar tarafından düzenli olarak denetlenmelidir. Gerekli tedbir ve önlemleri almayan ve ihmal eden sağlık kurum ve kuruluşlarına ve de medikal cihaz üretici firmalarına çeşitli cezalar ve yaptırımlar yapılmalıdır. Medikal cihazların güvenliği konusunda çok daha fazla çalışma ve araştırma yapılması gerekmektedir.

KAYNAKLAR

1. Harries D.,& Yellowless, P. M. (2014) Cyberterrorism: Is the U.S. Healthcare System Safe? Telemedicine and e-Health, 61-66
2. Hall, Susan D. Report: Healthcare the least prepared sector against cyberattacks. Yayın Tarihi: 20 Ocak 2016
3. http://www.tdk.gov.tr/index.php?option=com_karsilik&arama=kelime&guid=TDK.GTS.573e09ee1e23c2.15324266
4. Peraklis, E.D. (2014, 4 31). Cybersecurity in Health Care. Retrieved 5 20, 2016
5. Filkiins, B (2014, 2).Health Care Cyberthreat Report Widespread. Retrieved 5 20, 2016, from The SANS Institute
6. Hall, Susan D. Report: Healthcare the least prepared sector against cyberattacks. Yayın Tarihi: 20 Ocak 2016
7. Dvorak, Katie. Loss of life, liability top cybersecurity fears for health IT leaders. Yayın Tarihi: 21 Ocak 2016.
8. Finkle, J (2014, 10 22). Reuters. Retrieved 5 20, 2016, from U.S goverment probes medical devices for possible cyber flaws
9. http://lepicallidus.com/teknoloji/siber-guvenlikte-yeni-sorun-medikal-cihazlar
10. FDA. Vulnerabilities of Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems: FDA Safety Communication. Yayın Tarihi: 13 Mayıs 2015
11. Roberts, P. (2013, 5). Dexter Does AppSec: Life Or Death Matters in Medical Device Security
12. Strickland, Eliza. (2016, 15 Mart). 5 Major Hospital Hacks: Horror Stories from the Cybersecurity Frontlines
13. Security and Privacy for Implantable Medical Devices Daniel Halperin, Thomas S. Heydt-Benjamin, Kevin Fu, Tadayoshi Kohno, and William H. Maisel Vol. 7, No. 1 January-March 2008
14. http://www.haberturk.com/saglik/haber/1241415-anonymous-turkiyedeki-saglik-kayitlarini-caldi-mi
15. http://www.btnet.com.tr/guvenlik/medtronic%E2%80%99e-sizildi-saglik-verileri-calindi/1/16862
16. http://h4cktimes.com/analiz-makaleler/tibbi-cihazlarin-hacklenmesi.html
17. FDA. Postmarket Management of Cybersecurity in Medical Devices. Yayın Tarihi: 22 Ocak 2016.

18. FDA. Content of Premarket Submissions for Management of Cybersecurity in Medical Devices. Yayın Tarihi: 2 Ekim 2014.
19. FDA. Guidance for Industry Cybersecurity for Networked Medical Devices Containing Off the-Shelf (OTS) Software. Yayın Tarihi: 14 Ocak 2005.
20. Haigh, Tom; Landwehr, Carl. IEEE Cybersecurity, Building Code for Medical Device Software Security.
21. Bowman, Dan. Omnibus funding bill requires HHS to convene cybersecurity taskforce. Yayım Tarihi: 16 Aralık 2015.
22. Eastwood, Brian. 8 best practices for payer data security. Yayım Tarihi: 09 Şubat 2015
23. IBM X-Force Research. Security trends in the healthcare industry. New risks and priorities for keeping patient information safe. Erişim tarihi: 02 Ocak 2015.
24. https://sba.saglik.gov.tr/dosya/1-96380/h/201451993.pdf